HP B–series Fabric OS 6.3.2e Release Notes

HP Part Number: 5697-1816
Published: March 2012
Edition: 1

© Copyright 2010–2012 Hewlett-Packard Development Company, L.P.
© Copyright 2010–2012 Brocade Communications Systems, Incorporated

Contents

Version....5
Description....5
Update recommendation....5
Supersedes....5
Enhancements....5
Bottleneck Detection and Related Fabric Diagnostics enhancements....5
Optionally licensed software....6
Included licensed software....7
Temporary license support....8
Previously licensed software now included with base Fabric OS....8
Standards compliance....9
New hardware support....9
Supported product models....9
Unsupported product models....10
Devices supported....10
Operating systems....10
Access Gateway support....10
Access Gateway support in non-Brocade fabrics....11
Zoning and fabric operations....11
Prerequisites....12
4/256 SAN Director blade support....14
DC SAN Backbone and DC04 SAN Director blade support....15
Power supply requirements for Director blades....15
Fibre Channel Routing scalability....16
Important notes....16
New OUI Support on B-series platforms....16
Overview....16
Impact of products with the new OUI to existing fabrics/environments....17
HP SAN Network Advisor compatibility....17
DCFM compatibility....17
EFCM and FM compatibility....18
Fabric OS compatibility....18
Web Tools compatibility....19
Fabric OS feature compatibility in native connectivity modes....19
Firmware upgrades and downgrades....21
Firmware upgrade instructions....22
Scalability....22
Important notes and recommendations....22
HP Storage Essentials support....22
FCIP, FCIP Trunking and High Bandwidth (1606 Extension SAN Switch and DC SAN Director Multiprotocol Extension Blade)....22
FCoE/CEE (2408 FCoE Converged Network Switch and DC SAN Director Switch 10/24 FCoE Blade)....24
Virtual Fabrics....26
Licensing behavior....26
Adaptive Networking/flow-based QoS prioritization....26
FCR backbone fabric ID changes....27
Traffic Isolation over FCR....27
IP over Fibre Channel (IPFC)/FCR....27
Broadcast frame forwarding in FCR fabric....27
FC Routing with Mi10K....27
Integrated routing....28

FC FastWrite....28
Native connectivity....28
FCS Automatic Distribution....28
FCAP....28
FICON....28
FL_Port (loop) support....29
Port Mirroring....29
10Gb interoperability....29
Port Fencing....29
Zoning....30
ICLs....30
Extended Fabrics and R_RDY flow control....30
Implementation....30
8-Gb link initialization and fill words....31
Overview....31
portcfgfillword behavior summary....31
Miscellaneous....33
Encryption behavior....34
Initial setup of encrypted LUNs....39
Documentation Updates....40
Brocade Fabric OS Command Reference (Publication Number 53-1001337-01)....40
Brocade Fabric OS Encryption Administrator's Guide (Publication Number 53-1001760-011001341-02)....40
Fabric OS 6.3.2 fixes....40
Fabric OS 6.3.2a fixes....45
Fabric OS 6.3.2b fixes....47
Fabric OS 6.3.2c fixes....49
Fabric OS 6.3.2d fixes....51
Fabric OS 6.3.2e fixes....51
Effective date....52

Version

6.3.2e

NOTE: This software conforms to the Fibre Channel (FC) standards and accepted engineering practices and procedures.

Description

Fabric OS 6.3.2e is a patch release based on Fabric OS 6.3.2. All hardware platforms and features supported in Fabric OS 6.3.2 are also supported in version 6.3.2e. This release contains several fixes since the 6.3.2 release. Fabric OS 6.3.2a added a new CLI command as documented in the section titled (page 33) in these release notes.

Update recommendation

All products supported by Fabric OS 6.0.x can be upgraded to Fabric OS 6.3.2e, with the exception of the following switches:

- HP 4/8 SAN Switch
- HP 4/16 SAN Switch
- Brocade 4Gb SAN Switch for HP p-Class BladeSystem
- Brocade 4Gb SAN Switch for HP c-Class BladeSystem

If applicable, HP recommends that you upgrade to Fabric OS 6.3.2e as soon as possible to take advantage of the latest fixes and features.

For more information, see "Firmware upgrades and downgrades" (page 21).

Supersedes

Fabric OS 6.3.2d, released July 2011

Enhancements

Fabric OS 6.3.2 included several chassis management features for the Brocade 8Gb SAN Switch for HP BladeSystem c-Class switch. These changes allow configuration of Access Gateway mode and port mappings, and provides asynchronous notifications to chassis management software if the AG configuration is changed from CLI or Web Tools interfaces. Fabric OS 6.3.2a added a new CLI command, as documented in the section titled (page 33) in these release notes.

Bottleneck Detection and Related Fabric Diagnostics enhancements

Fabric OS 6.3.1b added several optional diagnostics enhancements that are also included in this version of Fabric OS. These enhancements are not fully documented in existing administrator guides or other materials, but will be captured in future updates and revisions. A brief summary of these enhancements follow:

- Identification of Virtual Channel (VC) stuck or credit lost condition and generation of RASLOG message (C2-5021) when detected. Unlike previous reporting that indicated when all credits for a VC were missing, this new capability reports on individual credit loss. This is enabled by default and is non-configurable.
- General improvements to Bottleneck Detection on both 4Gb and 8Gb platforms, including improved accuracy on reporting latency and reporting of latency values in Bottleneck Detection events.

- Addition of Class 3 frame transmit timeout discard counter support for 4Gb platforms. Previously, 4Gb platforms supported only receive (Rx) timeout counters. See the *Fabric Watch Administrator's Guide* for details on use and configuration.
- Addition of configurable "edge hold time" option to timeout frames for F_Ports sooner than for E_Ports. This option is disabled by default, but when enabled and properly configured, it reduces the likelihood of devices with high latencies causing frame drops in the core of the fabric and impacting other unrelated flows.

Optionally licensed software

Optionally licensed features in Fabric OS 6.3.2e are as follows:

- **Ports on Demand**—Allows customers to instantly scale the fabric by provisioning additional ports through a license key upgrade (applies to select switch models).
- **Extended Fabrics**—Provides greater than 10 km of switched fabric connectivity at full bandwidth over long distances. (Depending on the platform, the distance can be up to 3,000 km.)
- **ISL Trunking**—Enables aggregation of multiple physical links into one logical link for enhanced network performance and fault tolerance. It also includes Access Gateway ISL Trunking on the products that support the Access Gateway deployment.
- **Advanced Performance Monitoring**—Enables performance monitoring of networked storage resources. This license includes the Top Talkers feature.
- **High-Performance Extension over FCIP/FC** (formerly known as FC-IP Services)—For the HP B-series Multiprotocol Router Blade and 400 MP Router, this license key also includes the FC FastWrite (FCFW) feature and IPsec capabilities.
- **Accelerator for FICON license**—Enables unique FICON emulation support for IBM's Global Mirror (formerly XRC) application (including Hitachi Data Systems' HXRC and EMC's XRC), as well as tape pipelining for all FICON tape and virtual tape systems to significantly improve XRC and tape backup/recovery performance over virtually unlimited distance for the 400 MP Router and B-series Multiprotocol Router Blade.
- **Fabric Watch**—Monitors mission-critical switch operations, and now includes new Port Fencing capabilities.
- **FICON Management Server** (also known as the control unit port [CUP])—Enables host control of switches in mainframe environments.
- **HP StorageWorks DC SAN Director ICL 16-link**—Provides dedicated high-bandwidth links between two DC SAN Backbone Director chassis, without consuming valuable front-end 8Gb ports. Each DC Backbone Director must have the ICL license installed in order to enable ICL connections (available on the DC Backbone Director only).
- **HP StorageWorks DC SAN Director ICL 8-Link**—This license activates all 8 links on ICL ports on a DC04 SAN Director chassis for connection of two DC04 directors, or half of the ICL bandwidth for each ICL port on the DC SAN Backbone Director platform by enabling only 8 of the 16 links available. This allows users to purchase half the bandwidth of DC SAN Backbone Director ICL ports initially, and then upgrade with an additional 8-link license to utilize the full ICL bandwidth.

  This license is also useful for environments in which you want to create ICL connections between a DC SAN Backbone Director and a DC04 SAN Director. (The DC04 SAN Director can support only 8 links on an ICL port.) This license is available on the DC04 SAN Director and DC SAN Backbone Director platforms only. It replaces the original ICL license for the DC04 SAN Director and is new for the DC SAN Backbone Director.
- **Adaptive Networking**—Ensures high-priority connections and obtains the network resources necessary for optimum performance, even in congested environments. The QoS SID/DID

Prioritization and Ingress Rate Limiting features are the first components of this license and are available on all 8Gb platforms.

- **Integrated Routing license**—Allows ports on a DC SAN Backbone Director, DC04 SAN Director, 1606 Extension SAN Switch, HP 8/80 SAN Switch, or HP 8/40 SAN Switch to be configured as EX_Ports, supporting FCR. This eliminates the need to add a B-series Multiprotocol Router Blade or to use the 400 MP Router for FCR purposes, it also provides double the bandwidth for each FCR connection (when connected to another 8Gb-capable port).
- **Encryption Performance Upgrade**—This license provides additional encryption processing power. The Encryption Performance License enables full encryption processing power on the HP Encryption SAN Switch or on all HP DC Switch Encryption blades installed in the DC SAN Backbone Director/DC04 SAN Director chassis.
- **Server Application Optimization license** (introduced with Fabric OS 6.2)—When deployed with Brocade HBAs, optimizes overall application performance for physical servers and virtual machines by extending virtual channels to the server infrastructure. Application-specific traffic flows can be configured, prioritized, and optimized throughout the data center infrastructure. This license is not supported on the HP 2408 FCoE Converged Network Switch.
- **1606 Extension SAN Switch Port Upgrade**—This license allows a 1606 Extension SAN Switch to enable 16 FC ports (instead of the base 4 ports) and 6 GbE ports (instead of the base 2 ports). This license is also required to enable additional FCIP tunnels and advanced capabilities, such as tape read/write pipelining. A 1606 Extension SAN Switch must have the Port Upgrade license installed to add FICON Management Server (CUP) or Advanced Accelerator for FICON.
- **Advanced Extension**—This license enables two advanced extension features: FCIP Trunking and ARL. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP circuits) via multiple 1-GbE or 10-GbE interfaces to provide a high-bandwidth FCIP tunnel and failover resiliency. Each FCIP circuit also supports four QoS classes (Class-F, Hi, Medium, and Low Priority), each as a TCP connection. The ARL feature provides a minimum bandwidth guarantee for each tunnel, with full utilization of the available network bandwidth without impacting throughput performance under high traffic load. This license is available on the 1606 Extension SAN Switch and DC SAN Backbone Director/DC04 SAN Director for the DC SAN Director Multiprotocol Extension Blade on an individual slot basis.
- **10-GbE FCIP**—This license enables the two 10-GbE ports on the DC SAN Director Multiprotocol Extension Blade. With this license, two additional operating modes (in addition to 10 1-GbE ports mode) can be selected:
  - 10 1-GbE ports and 1 10-GbE port
  - 2 10-GbE ports

  This license is available on the DC SAN Backbone Director/DC04 SAN Director for the DC SAN Director Multiprotocol Extension Blade on an individual slot basis.
- **Advanced FICON Acceleration**—This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the HP 1606 SAN Extension Switch and the HP SN8000B 8-Slot SAN Backbone Director Switch, HP SN8000B 4-Slot SAN Director Switch, HP StorageWorks DC SAN Backbone Director Switch, HP StorageWorks DC04 SAN Director Switch for the HP DC SAN Director Multiprotocol Extension Blade on an individual slot basis.

Included licensed software

- **Enhanced Group Management**—This license is included with all HP 8Gb switches. Enhanced Group Management enables full management of the device in a data center fabric, with

increased element management functionality and management task aggregation throughout the environment. This license is used in conjunction with the DCFM application software.

- **2408 FCoE Converged Network Switch FC Ports on Demand**—This license enables all eight FC ports on the 2408 FCoE Converged Network Switch.

IMPORTANT: Most 2408 FCoE Converged Network Switch units shipped with Fabric OS 6.1.2_cee1 did not include this license and must have it installed before upgrading to Fabric OS 6.3.0 or later. Failure to do so will result in the disabling of FC ports after the upgrade. Contact HP Support to obtain this license key if your 2408 switch does not already have it installed.

- **FCoE**—This license enables Fibre Channel over Ethernet functionality on the 2408 FCoE Converged Network Switch. Without the FCoE license, the 2408 FCoE Converged Network Switch is a pure Layer 2 Ethernet switch and will not support FCoE bridging or FCoE Forwarding (FCF) capabilities.

Temporary license support

HP now supports temporary licenses or Universal Temporary Licenses. To obtain the Universal Temporary Licenses, select the **Software Demo & Evaluation Downloads** option at the HP website: www.software.hp.com.

The following list of licenses are available as Universal Temporary licenses. This means that the same license key can be installed on any switch running Fabric OS 6.3 or later that supports the specific feature. Universal Temporary license keys can be installed only once on a particular switch, but can be applied to as many switches as desired. Temporary use duration (the length of time the feature is enabled on a switch) is provided with the license key. All Universal Temporary license keys have an expiration date beyond which the license can no longer be installed on any unit.

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license
- Fabric Watch license
- Integrated Routing license
- Server Application Optimization license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10 GbE license/10 Gbps FC license
- FICON Management Server (CUP) license
- Enterprise ICL license

Previously licensed software now included with base Fabric OS

The capabilities described in this section are included as part of the base Fabric OS. No additional purchase or licensing is necessary.

NOTE: Starting with Fabric OS 6.1, Advanced Zoning and Web Tools licenses are not necessary. These features are enabled automatically on all products running Fabric OS 6.1 or later.

Standards compliance

This software conforms to the FC standards and accepted engineering practices and procedures. In certain cases, HP might add proprietary supplemental functions to those specified in the standards. For a list of standards conformance, see the HP website: http://www.hp.com.

The 2408 FCoE Converged Network Switch and DC SAN Director Switch 10/24 FCoE Blade conform to the following Ethernet standards:

- IEEE 802.1D, Spanning Tree Protocol (STP)
- IEEE 802.1s, Multiple Spanning Tree
- IEEE 802.1w, Rapid Reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad, Link Aggregation with LACP
- IEEE 802.3ae, 10G Ethernet
- IEEE 802.1Q, VLAN Tagging
- IEEE 802.1p, Class of Service Prioritization and Tagging
- IEEE 802.1v, VLAN Classification by Protocol and Port
- IEEE 802.1AB, Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x, Flow Control (Pause Frames)

The following draft versions of the CEE and FCoE standards are also supported on the 2408 FCoE Converged Network Switch and DC SAN Director Switch 10/24 FCoE Blade:

- IEEE 802.1Qbb, Priority-based Flow Control
- IEEE 802.1Qaz, Enhanced Transmission Selection
- IEEE 802.1, DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- FC-BB-5, FCoE (Rev. 2.0.0, introduced with Fabric OS 6.3.0b)

New hardware support

No new hardware support is provided in Fabric OS 6.3.2e.

Supported product models

Fabric OS 6.3.2e is supported on the following product models:

- HP 4/32 SAN Switch (Brocade 4100)
- HP 4/32B SAN Switch (Brocade 5000)
- HP 4/64 SAN Switch (Brocade 4900)
- HP 4/256 SAN Director (Brocade 48000)
- HP 16 Port 4Gb SAN Director Blade (FC4-16)
- HP 32 Port 4Gb SAN Director Blade (FC4-32)
- HP 48 Port 4Gb SAN Director Blade (FC4-48)
- HP Multi-Protocol Router Blade (Brocade FR4-18i)
- HP iSCSI Director Blade (Brocade FC4-16IP), compatible with the 4/256 SAN Director *only* (not supported in the DC SAN Backbone Director or DC04 SAN Director)
- HP 8/8 and 8/24 SAN Switches (Brocade 300)
- HP 8/40 SAN Switch (Brocade 5100)
- HP 8/80 SAN Switch (Brocade 5300)

- HP 400 Multiprotocol Router (Brocade 7500)
- HP Encryption SAN Switch (Brocade BES)
- HP DC04 SAN Director (Brocade DCX-4S)
- HP DC SAN Backbone Director (Brocade DCX)
- HP SAN Director 16 Port 8Gb FC Blade (Brocade FC8-16)
- HP SAN Director 32 Port 8Gb FC Blade (Brocade FC8-32)
- HP SAN Director 48 Port 8Gb FC Blade (Brocade FC8-48)
- HP SAN Director 6 Port 10Gb FC ISL Blade (Brocade FC10-6)
- HP DC Switch Encryption FC Blade (Brocade FS8-18)
- HP EVA4400 Embedded Switch Module (Brocade 5410)
- Brocade 8Gb SAN Switch for HP BladeSystem c-Class (Brocade 5480)
- HP 1606 Extension SAN Switch (Brocade 7800)
- HP 2408 FCoE Converged Network Switch (Brocade 8000)
- HP DC SAN Director Switch 10/24 FCoE Blade (Brocade FCOE10-24)
- HP DC SAN Director Multiprotocol Extension Blade (Brocade FX8-24)

Unsupported product models

Any product models not listed in Supported product models (page 9) do not support Fabric OS 6.3.x.

Devices supported

For a list of supported devices, see the HP website:

http://www.hp.com/go/san

Operating systems

For a list of operating systems, see the HP website:

http://www.hp.com/go/san

Access Gateway support

Access Gateway is supported with Fabric OS 6.3.*x* for the following HP products only:

- Brocade 8Gb SAN Switch for HP BladeSystem c-Class (Brocade 5480)
- HP 8/24 SAN Switch (Brocade 300)
- HP 8/40 SAN Switch (Brocade 5100)
- HP 2408 FCoE Converfed Network Switch (Brocade 8000)

IMPORTANT: Although the 8/8 SAN Switch uses the same hardware as the 8/24 SAN Switch, it does not support Access Gateway because only the 8/24 switch has all ports licensed as required for Access Gateway support. Similarly, for the 8/40 switch to support Access Gateway mode, all ports must be licensed. If you are using DCFM to manage a fabric with a 2408 FCoE switch in Access Gateway mode, version 10.4.0 or later is required.

Access Gateway connectivity is supported by the switches listed in this section and also by the following B-series switches:

- HP 4/16 SAN Switch (Brocade 200e)
- HP 4/32 SAN Switch
- HP 4/32B SAN Switch
- HP 4/64 SAN Switch
- HP 4/256 SAN Director
- Brocade 4Gb SAN Switch for HP p-Class BladeSystem (Brocade 4012)
- Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024)
- HP 8/80 SAN Switch
- HP DC SAN Backbone Director
- HP DC04 SAN Director
- HP 400 Multiprotocol Router
- HP EVA4400 Embedded Switch Module
- HP 1606 Extension SAN Switch (Brocade 7800)

Access Gateway mode allows a switch to operate in `agmode`, which provides simplified connectivity between large numbers of servers and the SAN. Access Gateway leverages N_Port ID Virtualization (NPIV) to hide the complexity of the servers (both physical and virtual) attached to it, while allowing easy SAN connectivity. The edge fabric switch provides all fabric services, while Access Gateway connects to the edge switch by what appears as a host bus adapter (HBA) connection. This architecture allows the deployment of many additional servers without requiring a domain and the associated fabric rebuild traffic. Rebuild traffic is prevalent when switches are powered on, added, or removed from a fabric.

For more information, see the *Brocade Access Gateway Administrator's Guide*, available on http://www.hp.com/go/san.

Access Gateway support in non-Brocade fabrics

In addition to being supported in Brocade fabrics, Access Gateway is supported with switches running Fabric OS 6.3.2x for connectivity to the following:

- McDATA switches: M4400, M4700, and Mi10K running EOS 9.9.7 with Brocade Fabric OS 6.3.2x
- Cisco switches: MDS 9216A, MDS 9506, MDS 9509, MDS 9120, MDS 9140, MDS 9124, and MDS 9134 running SAN OS 3.3(2), 3.3(3), 3.3(4), 3.3(4a) and 3.3(5) with Brocade Fabric OS 6.3.2x
- Cisco switches: MDS9124, MDS9124e, and MDS 9134 NX-OS 4.1(3a), 4.2(3), and 4.2(5) with Brocade Fabric OS 6.3.2x
- Cisco switches: MDS 9216i running SAN-OS 3.3(1c) and NX-OS 4.1(1c), 4.2(3), and 4.2(5) with Brocade Fabric OS 6.3.2x

Zoning and fabric operations

When configuring zoning or other fabric-wide settings in a fabric that has products operating with different versions of Fabric OS, HP recommends that you perform the configuration through an interface (such as Web Tools) to a product with the most recent version of Fabric OS. Some older versions of Fabric OS do not fully support newer hardware models, and problems may arise when configuring settings through these older products.

NOTE: Do not configure zoning through a switch operating with Fabric OS 3.x in a fabric that has products operating with later versions of Fabric OS.

Prerequisites

Table 1 (page 13) lists the supported Fabric OS firmware versions. HP recommends using the latest supported firmware versions to get the greatest benefit from the SAN.

For a list of retired products, see the HP website:

http://www.hp.com

IMPORTANT: The Fabric OS versions listed in the **Earliest compatible version** column in Table 1 (page 13) are the earliest versions supported by HP for connection to switches running Fabric OS 6.3.2e at the time of its release.

Versions shown as supported in Table 1 (page 13) reflect support as of the date of the publication of these release notes. For the latest product support information, see the Single Point of Connectivity Knowledge (SPOCK) on the HP website: http://www.hp.com/storage/spock. You must sign up for an HP Passport to access this website.

Table 1 Supported Fabric OS versions

Model	Earliest compatible version	Recommended version
HP MSA SAN Switch 2/8	3.2.1c	3.2.1c[1,6,7]
HP SAN Switch 2/16 HP SAN Switch 2/8-EL HP SAN Switch 2/16-EL HP Core Switch 2/64 HP SAN Director 2/128 in Chassis Config modes 3 and 4 only	Not supported (support ended September 2009)	N/A
HP SAN Switch 2/8V HP SAN Switch 2/16V HP SAN Switch 2/32	Not supported (support ended N/A November 2010)	N/A
HP SAN Director 2/128	Not supported (support ended August 2011)	N/A
HP 4/8 SAN Switch HP 4/16 SAN Switch	6.2.2e	6.2.2f
HP 4/256 SAN Director HP 4/64 SAN Switch HP B-series MP Router Blade (FR4-18i)[8] HP 16 Port 4-Gb Blade (FC4-16) HP 32 Port 4-Gb Blade (FC4-32) HP 48 Port 4-Gb Blade (FC4-48) HP 400 MP Router[8] HP 4/32 SAN Switch HP 4/32B SAN Switch HP B-series iSCSI Director Blade (FC4-16IP)	6.2.2e	6.4.2b[5]
Brocade 4-Gb SAN Switch for HP p-Class BladeSystem Brocade 4-Gb SAN Switch for HP c-Class BladeSystem	6.2.2e	6.2.2f[5]
HP MP Router	XPath OS 7.4.1e (Not supported for connectivity to switches running Fabric OS 7.x)	XPath OS 7.4.1f[8]
HP DC SAN Backbone Director	6.3.2d	7.0.1
Brocade 8-Gb SAN Switch for HP BladeSystem c-Class	6.3.2d	7.0.1
HP EVA4400 Embedded Switch Module, 8-Gb Brocade	6.3.2d	7.0.1
HP DC04 SAN Director	6.3.2d	7.0.1
HP SAN Director 16 Port 8-Gb FC Blade (FC8-16) HP SAN Director 32 Port 8-Gb FC Blade (FC8-32) HP SAN Director 48 Port 8-Gb FC Blade (FC8-48)	6.3.2d	7.0.1
HP SAN Director 6 Port 10-Gb ISL Blade (FC10-6)	6.3.2d	7.0.1
HP 8/8 SAN Switch HP 8/24 SAN Switch HP 8/40 SAN Switch	6.3.2d	7.0.1

Table 1 Supported Fabric OS versions *(continued)*

HP 8/80 SAN Switch		
HP Encryption SAN Switch	6.3.2d	7.0.1
HP 1606 Extension SAN Switch (Brocade 7800)	6.3.2d	7.0.1
HP 2408 FCoE Converged Network Switch (Brocade 8000)	6.3.2d	7.0.1
HP DC SAN Director Switch 10/24 FCoE Blade (Brocade FCOE10-24)	6.3.2d	7.0.1
HP DC SAN Director Multiprotocol Extension Blade (Brocade FX8-24)	6.3.2d	7.0.1
HP DC Switch Encryption FC Blade	6.3.2d	7.0.1
Mi10k M4400, M4700 (McDATA Fabric Mode and Open Fabric Mode)[2, 4]	M-EOS 9.9.5[3]	M-EOS 9.9.8 or later[3]
Data Center Fabric Manager **NOTE:** DCFM does not support any 16 Gb products.	10.4.0	10.4.5a
HP Network Advisor	11.1.0	11.1.3

Table notes:

[1] All zoning and fabric operations in a fabric with products running older versions of Fabric OS should be performed using interfaces to products running the latest version of Fabric OS. This is important for Brocade 3*xxx* series switches that do not support zoning configuration for newer products.

[2] Other M-EOS models can participate in a fabric with Fabric OS 6.3, but cannot be directly attached via an E_Port to any products running Fabric OS 6.3. For information about HP support of interoperable fabrics, see *HP Merging Fabrics Based on M-series and B-series Fibre Channel Switches Application Notes*, available at http://www.hp.com.

[3] HP strongly recommends that M-EOS products operate with the most recent version of M-EOS that supports interoperability. M-EOS 9.9.5 is the only version that has been fully qualified for interoperability with Fabric OS 6.3. For information about HP support of interoperable fabrics, see *HP Merging Fabrics Based on M-series and B-series Fibre Channel Switches Application Notes*, available at http://www.hp.com.

[4] When routing to an M-EOS edge fabric using frame redirection, the fabric must have a Fabric OS-based product in order to configure the frame redirection zone information.

[5] When directly attached to a host or target that is part of an encryption flow.

[6] Products operating with Fabric OS versions earlier than 5.3.1b or 6.1.0e cannot participate in a logical fabric that is using XISLs (in the base fabric).

[7] These platforms cannot be directly attached to hosts or targets for encryption flows.

[8] SANRouters 1620 and 2640 should not be used with XPath or Fabric OS-based routing (FCR) for connections to the same edge fabric.

4/256 SAN Director blade support

Fabric OS 6.3.2e is fully qualified and supports only the Director blades listed in Table 2 (page 15).

Table 2 4/256 SAN Director blade support matrix

Director blade	Number of blades
FC4-16 FC4-32 FC4-48 FC8-16 FC8-32 FC8-48 FC10-6	Supported with any mix, with up to eight blades of each type. No intermix restrictions. The 4/256 SAN Director must run Fabric OS 6.0.0b or later to support the FC8-16 port blade, and Fabric OS 6.1.0a or later to support the FC8-32 and FC8-48 port blades.
FC4-16IP (iSCSI blade)	Up to four blades of this type
FR4-18i (FCIP/FC Router blade)	Up to two blades of this type. Up to eight FR4-18i blades can be installed if they are used only for FC FastWrite or FCIP without routing.

DC SAN Backbone and DC04 SAN Director blade support

Fabric OS 6.3.2e is fully qualified and supports the DC Director blades listed in Table 3 (page 15).

Table 3 DC Director blade support matrix

Director blade	Number of blades
FC8-16 FC8-32 FC8-48 FC10-6	Supported with Fabric OS 6.0.0b or later with any mix, with up to eight blades of each type on the DC SAN Backbone Director. There are no intermix restrictions. The DC04 SAN Director requires Fabric OS 6.2.0a or later, and supports up to four blades.
FC4-16IP (iSCSI blade)	Not supported with the DC SAN Backbone Director or DC04 SAN Director
FR4-18i (FCIP/FC Router blade)	Supported with Fabric OS 6.0.0b or later, with a maximum of four blades of this type on the DC SAN Backbone Director. Up to eight FR4-18i blades can be installed if they are used only for FC FastWrite or FCIP without routing on the DC SAN Backbone Director. The DC04 SAN Director requires Fabric OS 6.2.0a or later, and supports up to four blades.
FS8-18 (DC Switch Encryption FC blade)	Supported with Fabric OS 6.2.0b or later, with a maximum of four blades of this type on the DC SAN Backbone Director or DC04 SAN Director
FX8-24 (DC SAN Director Multiprotocol Extension Blade) FCOE10-24 (DC SAN Director Switch 10/24 FCoE Blade)	Supported with Fabric OS 6.3.0x, with a maximum of two blades per director. The DC SAN Director Switch 10/24 FCoE Blade can be installed in the same chassis only with FC8-*xx* and/or FC10-6 blades. It is not supported in the chassis with any other blades.

Power supply requirements for Director blades

Table 4 (page 16) lists power supply requirements for Director blades to provide full redundancy (220 VAC power is assumed).

IMPORTANT: Director blades must meet the minimum Fabric OS levels to operate in the Director chassis. For example, the FC8-32 is not supported in the 4/256 SAN Director with Fabric OS 6.0.x.

Table 4 Power supplies required for blades in Director chassis

Director blade	4/256 SAN Director	DC SAN Backbone Director and DC04 SAN Director
FC4-16 FC4-32 FC4-48 FC8-16 FC8-32	Two power supplies	Two power supplies[1]
FC8-48 FC10-6	Four power supplies	Two power supplies[2]
FR4-18i (FCIP/FC Router blade) FC4-16IP (iSCSI blade)	Four power supplies	Two power supplies. The FC4-16IP blades are not supported in the DC SAN Backbone Director or DC04 SAN Director.[2]
FS8-18 (DC Switch Encryption FC Blade) FX8-24 (DC SAN Director Multiprotocol Extension Blade) FCOE10-24 (DC SAN Director Switch 10/24 FCoE Blade)	Not supported	Two power supplies. For the DC SAN Backbone Director with three or more FS8-18 blades, (2+2) 220 VAC power supplies are required for redundancy. For one or two FS8-18 blades, only two power supplies are required for redundancy. For the DC04 SAN Director, only two 220 VAC power supplies are required for redundancy with any number of FS8-18 blades. For the DC SAN Backbone Director or DC04 SAN Director, only two 220 VAC power supplies are required for redundancy with FX8-24 blades.[2]

[1] The FC blades in this row are the only ones supported in the DC SAN Backbone Director or DC04 SAN Director with 110 VAC power supplies.

[2] 110 VAC is not supported in either the DC SAN Backbone Director or DC04 SAN Director with these blades.

Fibre Channel Routing scalability

For the latest information about Fibre Channel Routing (FCR) scalability support, see the *HP SAN Design Reference Guide*, available at:

http://www.hp.com/go/sandesignguide

Important notes

This section contains information that you should consider before you use this Fabric OS release.

New OUI Support on B-series platforms

Overview

The OUI (Organizationally Unique Identifier) value is part of a Fibre Channel WWN that uniquely identifies the manufacturer of Fibre Channel products. The OUI values assigned to Brocade are used by Fabric OS to validate certain fabric interoperability support.

The currently assigned OUI/WWN values have been exhausted, necessitating Brocade to use a new OUI value for WWN assignment. The new OUI value for Brocade is `00:05:33`. A WWN of `10:00:`**`00:05:33`**`:41:5c:c1`, for example, demonstrates the usage of the new OUI.

Fabric OS 6.3.1a and later has been enhanced to recognize the new Brocade OUI value to guarantee proper functionality. It is important to note that no switch with the new OUI/WWN

should be downgraded to a version of Fabric OS that does not recognize this new OUI. It is also important to note that specific minimum requirements for recognition of the new OUI will neither be validated nor enforced by Fabric OS.

Impact of products with the new OUI to existing fabrics/environments

In most situations, a switch that uses the new OUI can be seamlessly added to an existing fabric, even if the other switches in that fabric are not using Fabric OS versions that are aware of the new OUI value. However, there are some exceptions and limitations to consider before adding a switch utilizing the new OUI to an existing fabric or environment.

- **Fabrics with encryption products:** If an HP encryption switch or blade using the new OUI is added to an edge fabric of a Fibre Channel routed fabric, Frame Redirection capability could be impacted across the FCR backbone, thus impacting the encryption functionality. Therefore, the FC routers in the FCR backbone fabric will need to be upgraded to a firmware version that supports the new OUI.
- **Interopmode 2 and 3 fabrics:** In an interopmode 2 or 3 fabric with VE ports, the switches on both ends of the VE link must run a firmware version that supports the new OUI, or the VE ports may not function correctly, resulting in unpredictable behavior.

HP SAN Network Advisor compatibility

HP SAN Network Advisor is a comprehensive SAN management application that enables end-to-end management of HP B-series data center fabrics. It is the next generation product and the successor to Data Center Fabric Manager (DCFM). HP Network Advisor is available in three versions (see the HP Network Advisor release notes for full support details):

- HP Network Advisor Professional is an application bundled with B-series switches that is ideally suited for small- and medium-size businesses that need a lightweight management product to manage their smaller fabrics (one physical fabric at a time, up to 1,000 ports). HP Network Advisor Professional supports DC04 SAN Director, and 4/256 SAN Director (but not DC SAN Backbone Director), FC switches, FCIP switches, FCR switches/Integrated Routing (IR) capabilities, FCoE/CEE switches, and Brocade HBAs.
- HP Network Advisor Professional Plus is a SAN management application designed for medium-size businesses to manage up to four physical Fabric OS fabrics and up to 2,560 switch ports. HP Network Advisor Professional Plus supports DC04 SAN Director and 4/256 SAN Director, FC switches, FCIP switches, FCR switches/Integrated Routing (IR) capabilities, FCoE/CEE switches, encryption switch and blade, and Brocade HBAs. Enterprise class customers who want to manage departmental SANs can consider deploying this product.
- HP Network Advisor Enterprise is an application designed for enterprise-class customers that provides unparalleled performance and scalability (24 physical fabrics, up to 9,000 switch ports). HP Network Advisor Enterprise configures and manages the same switches and directors as Professional and Professional Plus, but also adds support for the DC SAN Backbone Director. HP Network Advisor Enterprise is required to manage FICON fabrics. Existing DCFM customers that have active Maintenance and Support contracts are provided a seamless migration path to HP Network Advisor Enterprise.

DCFM compatibility

Fabric OS 6.3.2e is fully compatible with DCFM 10.4.x management software. DCFM is a comprehensive SAN management application that enables end-to-end management of HP B-series data center fabrics. With the introduction of HP Network Advisor, DCFM has been put into sustaining mode. DCFM is not qualified or supported for management of switches operating with Fabric OS 7.0.0a and later firmware versions.

IMPORTANT: You must first upgrade DCFM to Network Advisor 11.1.0 or later if you are planning to upgrade devices to Fabric OS 7.0.0a, or you risk losing management connectivity.

DCFM is available in three versions (see the DCFM release notes for full support details):

- **DCFM Professional**—An application bundled with B-series switches that is ideally suited for small- and medium-size businesses that need a lightweight management product to manage their smaller fabrics (one physical fabric at a time, up to 1,000 ports).
- **DCFM Professional Plus**—A SAN management application designed for medium-size businesses to manage up to four physical fabrics (Fabric OS, M-EOS, and mixed fabrics) and up to 2,560 switch ports. DCFM Professional Plus supports Brocade director products (for example, DC04 SAN Director and 4/256, but not DC SAN Backbone Director), FC switches, FCIP switches, FCR switches/Integrated Routing (IR) capabilities, FCoE/CEE switches, and Brocade HBAs. Enterprise-class customers who want to manage departmental SANs can consider deploying this product.
- **DCFM Enterprise**—An application designed for enterprise-class customers that provides unparalleled performance and scalability (24 physical fabrics, up to 9,000 switch ports). DCFM Enterprise configures and manages DC SAN Backbone Directors, along with other B-series directors, routers, switches, and HBAs. DCFM Enterprise is required to manage FICON fabrics, and fabrics with the DC SAN Backbone Director. Existing EFCM and FM customers that have active Maintenance and Support contracts are provided a seamless migration path to DCFM Enterprise.

NOTE: Beginning with version 10.4.0, DCFM provides limited management of Fabric OS switches or fabrics using Administrative Domains (ADs). Environments using ADs must use DCFM 10.4.0 or later, or use the CLI or Web Tools for management. See the *DCFM 10.4.0 User Guide* for details. When managing a 2408 FCoE Converged Network switch in Access Gateway mode, DCFM 10.4.0 or later is required. Use of earlier DCFM releases prevents management of zoning on the fabric.

EFCM and FM compatibility

With the introduction of DCFM, both EFCM and FM have been put into sustaining mode. Consequently, neither EFCM nor FM are qualified or supported to manage switches operating with Fabric OS 6.3.*x* firmware. Significant compatibility issues exist between FM and Fabric OS 6.3.*x*, including (but not limited to) compromised functionality in the zoning dialog and performance graphs, port enabling/disabling, and FICON wizard. HP strongly recommends that customers migrate from these products to DCFM.

Fabric OS compatibility

Table 1 (page 13), "Supported Fabric OS versions," lists the earliest versions of software supported in this release, that is, the earliest supported software versions that interoperate. HP recommends using the latest software versions to get the greatest benefit from the SAN.

When using the Virtual Fabrics (VF) feature, HP recommends that all switches participating in a fabric with a logical switch use the latest firmware available. All switches must be operating at the minimum firmware levels or later, as noted in the Fabric OS Interoperability table.

When using either the Encryption SAN Switch or DC Switch Encryption FC Blade, switches attached to hosts and targets on switches that are part of the encryption flow must operate at the following minimum levels:

- 2-Gb platforms must operate with Fabric OS 5.3.2b or later.
- 4-Gb and 8-Gb platforms must operate with Fabric OS 6.2.2f, 6.3.2d or later.

Web Tools compatibility

- Fabric OS 6.3 is supported with JRE 1.6.0 Update 13.
- If the JRE 1.6.0 version is not Update 13, the DCFM server/client and B-series Element Manager (Web Tools) crashes on launch.
- Web Tools tunnel and TCP graphs support tool tips only for the first enabled TCP connection graph.

Fabric OS feature compatibility in native connectivity modes

Some Fabric OS features are not fully supported when operating in the native connectivity modes for deployment with M-EOS-based products. All HP models supported by Fabric OS 6.3.2e support both interopmodes 2 and 3, with the exception of the 4/32 SAN Switch, 2408 FCoE Converged Network Switch, and DC SAN Backbone Director or DC04 SAN Director with one or more DC SAN Director Switch 10/24 FCoE Blades.

NOTE: HP may not support all of these switches in this mode. For information about support in interopmodes 2 and 3, see *HP Merging Fabrics Based on M-Series and B-Series Fibre Channel Switches Application Notes*, available at http://www.hp.com.

Table 5 (page 19) specifies Fabric OS feature support when operating in either interopmode 2 (McDATA Fabric Mode) or interopmode 3 (Open Fabric Mode) with Fabric OS 6.3.2e.

Table 5 Feature support in interopmodes 2 and 3

Fabric OS features (supported in interopmode 0)	Fabric OS 6.3.2e	
IM = interopmode	IM 2	IM 3
L2 Fabric OS Hot Code Load	Yes	Yes
Fabric OS Hot Code Load with FCR	Yes	Yes
Zone Activation Support	Yes	Yes[11]
Traffic Isolation Zones[1]	Yes	No
Frame Redirection (devices attached to Fabric OS)[1]	Yes	Yes[11]
Frame Redirection (devices attached to M-EOS)[1]	Yes	Yes[11]
Frame Redirection over FCR[10]	Yes	Yes[11]
FCR Fabric Binding (route to M-EOS fabric with Fabric Binding)[9]	Yes	Yes
L2 Fabric Binding	Yes	No*
DCC policies	No	No
SCC policies	Yes[4]	No*
E/EX_Port Authentication	Yes	Yes
ISL Trunking (frame level)	Yes[2]	Yes[2]
Dynamic Path Selection (DPS, exchange-based routing)	Yes[3]	Yes[3]
Dynamic Load Sharing (DLS, port-based routing)	Yes	Yes
Virtual Channels (VC RDY)	Yes[2]	Yes[2]
FICON Management Server (Cascading)	Yes	No*
FICON MIHPTO	Yes	No*
Full Scalability (to maximum M-EOS fabric limits)	Yes	Yes

Table 5 Feature support in interopmodes 2 and 3 *(continued)*

Adaptive Networking QoS	No	No
Adaptive Networking: Ingress Rate Limiting	No*	No*
Advanced Performance Monitoring (APM)	No*	No*
APM: Top Talkers	No*	No*
Admin Domains	No	No
Secure Fabric OS[5]	N/A	N/A
Fabric Watch	Yes	Yes
Ports on Demand (POD)	Yes	Yes
NPIV	Yes	Yes
Timer Server Function (NTP)	No	No
Open E_Port[6]	N/A	N/A
Broadcast Zoning	No	No
FDMI	No	No
Remote Switch	No	No
Port Mirroring	Yes	Yes
Extended Fabrics	Yes	Yes[7]
Alias Server	No	No
Platform Service	No	No
FCIP (VE_Ports)	Yes	Yes
IPFC (IP over FC)	Yes[8]	Yes[8]
M-EOS ALPA 0x13 configuration	Yes	Yes
VE_Port to VEX_Port	Yes	Yes
Integrated Routing[9]	Yes	Yes
Domain Offset Support	Yes	Yes
239 Domain Support (available on Mi10K only)	N/A	Yes
Masterless F_Port Trunking (AG connect to Fabric OS switches only)	Yes	Yes
FC10-6 to FC10-6 ISL	Yes	Yes
RASLog Events on Duplicate WWNs	Yes	Yes
Virtual Fabrics	Yes	Yes
Logical Fabric using LISLs (XISLs in base Fabric)	No	No
Port Fencing	Yes	Yes
Bottleneck Detection	Yes	Yes

*The feature is available, but not tested or supported.

[1]Requires M-EOS 9.7 or later for redirection between devices attached to Fabric OS switches, M-EOS 9.8 for redirection between devices attached to M-EOS switches, M-EOS 9.9 for use in McDATA Open Fabric Mode. Supported EOS platforms include M4400, M4700, M6140, and Mi10K.

[2]Allowed only between Fabric OS-based switches.

[3]DPS is supported outbound from Fabric OS-based switches. M-EOS can provide reciprocal load balancing using Open Trunking.

[4]SCC policies are supported only in conjunction with L2 Fabric Binding.

[5]Not supported in Fabric OS 6.0 or later.

[6]Mode 3 is qualified only with M-EOS switches.

[7]Not on FCR.

[8]Supported only locally on the Fabric OS switch.

[9]All routers (EX_Ports) must reside in a backbone fabric running in interopmode 0 only. Only edge fabrics with devices imported to the backbone fabric or other edge fabrics can operate in interopmode 2 or 3.

[10]To support Frame Reduction to an M-EOS edge fabric, there must be at least one Fabric OS switch in the edge fabric to configure Frame Redirection zones.

[11]Only Frame Reduction zones can be configured on Fabric OS platforms and sent to fabrics operating in McDATA Open Fabric Mode (interopmode 3). M-EOS 9.9 is required to support Frame Reduction zones in McDATA Open Fabric Mode.

NOTE: FICON Cascaded CUP is qualified on select platforms only.

Firmware upgrades and downgrades

Upgrading to Fabric OS 6.3.2e is allowed only from Fabric OS 6.2.0a or later. The policy to support one-level migration only, which began with Fabric OS 6.0.0, provides more reliable and robust migrations. By having fewer major changes in internal databases, configurations, and subsystems, the system can perform the upgrade more efficiently, ensuring a truly seamless and nondisruptive process for the fabric. The one-release migration policy also reduces the number of upgrade-downgrade permutations that must be tested, allowing for thorough testing and verification of supported migration paths.

If migrating from Fabric OS 6.1.x, HP recommends that you use Fabric OS 6.2.2b or later 6.2.x release as the migration path to 6.3.2e in order to reduce the risk of exposure to known issues at earlier 6.2.x levels.

The 2408 FCoE Converged Network Switch does not support nondisruptive Hot Code Loads (HCLs). As a result, any firmware upgrades are disruptive to the I/O through the switch. Similarly, a code load of DC SAN Director or DC04 SAN Director with one or more DC SAN 10/24 FCoE blades disrupts traffic through the blade.

When upgrading a 2408 FCoE Converged Network Switch from Fabric OS 6.1.2_cee1 to 6.3, verify that the unit has both the FCoE and FC POD licenses installed (default for HP 2408 switches). Units missing these licenses that are upgraded to Fabric OS 6.3 will lose functionality following a restart or disabling of ports. When the FC POD license is installed on a unit with Fabric OS 6.1.2_cee1, the `licenseShow` output will indicate that the license is `not applicable on this platform`. This message can be ignored and will not appear once the unit has been upgraded to Fabric OS 6.3.

If a Fabric OS 6.2 switch is in the Federal Information Processing Standards (FIPS) mode, and has only LDAP authentication support, and is upgraded to Fabric OS 6.3, login will fail. Therefore, if the 6.2 switch is in the FIPS mode, you should configure both LDAP and local authentications before upgrading it to Fabric OS 6.3. When the switch is up, you can log in to the switch and import the certificate again. If the switch is not in the FIPS mode, you can log in to the switch with LDAP after upgrading to Fabric OS 6.3, and then import the certificate.

Fabric OS 6.3x does not support concurrent FC Routing (EX_Ports) and Top Talkers features. Upgrading to Fabric OS 6.3x requires that one of these features be disabled first.

If there are multiple node encryption groups (EGs) in a fabric, complete the firmware download on one node at a time before downloading on another node.

Firmware upgrade instructions

IMPORTANT: HP recommends that you upgrade to Fabric OS 6.3.2e as soon as possible to take advantage of the fixes and new features. Upgrading to Fabric OS 6.3.2e is allowed only from Fabric OS 6.2.x. For more guidelines, see Update recommendation .

To access the latest Fabric OS 6.3.2e firmware, configuration files, and MIB files, see the HP website:

http://www.hp.com/support/downloads

On the website:

1. Under Storage, select **Storage Networking**.
2. Select the link for the appropriate switch, select your product, and then select **Cross operating system (BIOS, firmware, Diagnostics, etc.)**.
3. Select **Firmware**.
4. Select **V6.x Firmware** for HP B-series Fibre Channel Switches for Fabric OS 6.3.2e.
   - To download the firmware, click **Download**.
   - To read the release notes, click the **Release Notes** tab.

To verify that the firmware download is complete, enter the `firmwareDownloadStatus` command on the switch, verify that the process is complete, and then proceed to the next switch.

Scalability

For details on supported scalability, see the *HP SAN Design Reference Guide*, available on the HP website:

http://www.hp.com

Important notes and recommendations

This section contains additional information that you should consider before you use this Fabric OS release.

HP Storage Essentials support

HP Storage Essentials SAN management application 6.1.1 or later is supported with Fabric OS 6.3*x*. Earlier versions of HP Storage Essentials are not supported with Fabric OS 6.3*x* due to the incompatibility of Storage Essentials with the SMI-S 120.10.0 agent.

FCIP, FCIP Trunking and High Bandwidth (1606 Extension SAN Switch and DC SAN Director Multiprotocol Extension Blade)

- The 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade supports a maximum MTU size of 1500 with Fabric OS 6.3x.
- FCIP connections are supported only between the 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade and another 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade. FCIP tunnels are not supported between the 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade and the previous generation HP 400 Multiprotocol Router and HP Multiprotocol Router Blade platforms.
- When additional circuits (and the network bandwidth provided by those circuits) are added to an already active tunnel, there is a short period where some frame loss can occur due to the process to refresh the internal FC frame routing tables in the switch. Therefore, additional circuits should be added only during low I/O periods using the FCIP tunnel being modified. In addition, if the circuit operation (addition/deletion) to the tunnel increases or decreases the total tunnel bandwidth, an FCIP tunnel (VE_Port) disable/enable sequence should be performed

after the addition or deletion of the circuit. This allows the switch to adjust the internal routes to fully utilize the new bandwidth.

- Switching modes between 10G and 1G is disruptive to FCIP traffic.
- Keep Alive Timeout (ms). The valid range is 500 ms to 7,200,000 ms (inclusive). The default value is 10,000 ms (10 seconds). If FICON is configured, the recommended value is 1000 ms (1 second), otherwise the recommended value is the default of 10 seconds. For impairment networks with 100 ms latency and 0.5% packet loss, Keep Alive Timeout should be configured as 30 seconds. If the local and remote circuit configurations' Keep Alive Timeout values do not match, the tunnel will use the lower of the two configured values.
- Software compression (available on the 1606 Extension SAN Switch) modes 2 and 3 are not supported in FICON environments; they are supported only in Open Systems environments.
- Software compression (modes 2 and 3) generally gives a better compression ratio, but not the throughput or bandwidth across all six GE ports. HP recommends software compression for low-throughput links and supports throughput up to 2 Gb/s across all 6 GE ports.
- To perform the following operations you must delete the FCIP configuration on the affected ports first:
  - Switching modes between 1G/10G/Dual
  - Moving VE/GE port between logical switches
- The DC SAN Director Multiprotocol Extension Blade supports three operating modes:
  - Mode 1: 10 1-GbE ports mode (default)
  - Mode 2: 10 1-GbE ports and 1 10-GbE port
  - Mode 3: 2 10-GbE ports

  Modes 2 and 3 require the slot-based 10-GbE FCIP license.
- ARL (Adaptive Rate Limiting) is not supported on 10-Gb tunnels.
- IPv6, DiffServ, and In-band Management are not supported on the 1606 Extension SAN Switch or DC SAN Director Multiprotocol Extension Blade .
- IPSec is not supported on the DC SAN Director Multiprotocol Extension Blade.
- Fabric OS 6.3 supports only up to four 1-Gb circuits per VE/FCIP tunnel for the 1-Gb interfaces. A VE/FCIP tunnel created over 10-Gb interfaces will be limited to 10 circuits created using IPIFs on the same 10-GbE port (and no more than 1 Gb per circuit).
- As a recommended best practice, the VE tunnel should not be oversubscribed (for example, 8-Gb FC traffic over 500 Mb/s tunnel). General guidelines are 2:1 subscription without compression and 4:1 with compression.
- Nondisruptive firmware activation on Fabric OS 6.3 will disrupt I/O traffic on FCIP links.
- FCR (VEX) is not supported on the DC SAN Director Multiprotocol Extension Blade but is supported on the 1606 Extension SAN Switch.
- Differences between the 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade platforms and previous-generation 7500/FR4-18i platforms include:
  - On the 1606 Extension SAN Switch, the GigE port does not directly correlate to a VE_Port.
  - On the DC SAN Director Multiprotocol Extension Blade, GigE ports 0-9 or 10-GbE port 1 (xge1) correspond to VE_Ports 12-21, and 10-GbE port 0 (xge0) corresponds to VE_Ports 22-31.
  - The CLI syntax for the 1606 Extension SAN Switch/DC SAN Director Multiprotocol Extension Blade varies from the 7500/FR4-18i. See the *Brocade Fabric OS Command Reference* document for Fabric OS 6.3 for details.

- Both ends of a tunnel must be identically configured for the Compression, FastWrite, and Tape Pipeline options. If a mismatch exists, the tunnel will not be established and the TCP virtual connections will be removed.
- Under traffic isolation (TI) zone configurations with failover enabled, non-TI zone traffic will use the dedicated path if no other E or VE paths through the fabric exist, or if the nondedicated paths are not the shortest paths. (A higher bandwidth tunnel with multiple circuits will become the shortest path compared to a single tunnel.)
- A VE/VEX tunnel and E/EX FC port cannot connect to the same domain at the same time.
- The recommended Keep Alive Timeout must be the same on the tunnel and circuits on the switches on both sides of a link.
- Latency measurements supported on FCIP tunnels (tested limit under Fabric OS 6.3.2):
  - 1 GbE with 200 ms round-trip time and 1% loss
  - 10 GbE with 50 ms round-trip time and 0.1% loss
- The 1606 Extension SAN Switch supports optical and copper media types on GE0 and GE1 interfaces. Copper media is the default on GE0/GE1 ports and does not support autosense functions.
- Inserting a 4 Gb SFP in GE ports of an HP 1606 Extension SAN Switch or DC SAN Director Multiprotocol Extension Blade, can occasionally return one of the following messages:
  - `No_Light` or `Unknown` for GE ports in `switchshow` output.

    Remove and reinsert the optic cable to correct this indication.
  - `Can't read serial data` in `sfpshow` output.

    Reissue the `sfpshow` command to resolve this issue.

FCoE/CEE (2408 FCoE Converged Network Switch and DC SAN Director Switch 10/24 FCoE Blade)

- `Configupload` and `configdownload` operations attempted on the 2408 FCoE Converged Network Switch fail with an error message if that switch does not have an FCoE license installed and is running a firmware version earlier than Fabric OS 6.4.0c.
- The 2408 FCoE Converged Network Switch balances the FCoE bandwidth across all six port groups (each port group contains four ports). To get optimum performance for FCoE traffic HP recommends that the user distribute server CNA connections across these six port groups.
- Hot-plugging a CP with a firmware level earlier than Fabric OS 6.3.0 into a DC SAN Backbone Director or DC04 SAN Director with an active DC SAN Director Switch 10/24 FCoE Blade will result in the new standby CP not being HA synchronized. To avoid this scenario, upgrade the code on the standby CP directly to match the version on the active CP.
- HP recommends that Converged Mode be enabled on all interfaces connected to CNAs.
- When operating in Converged Mode, tagged traffic on the native VLAN of the switch interface is processed normally. The host should be configured not to send VLAN tagged traffic on the switch's native VLAN.
- The CNA may lose connectivity to the 2408 FCoE Converged Network Switch/DC SAN Director Switch 10/24 FCoE Blade if the CNA interface is toggled repeatedly over time. This issue is related to the CNA; rebooting the CNA restores connectivity.
- Although the 2408 FCoE Converged Network Switch/DC SAN Director Switch 10/24 FCoE Blade support the configuration of multiple CEE maps, HP recommends that you use only one CEE map on all interfaces connected to CNAs. Additionally, CEE maps are not recommended for use with non-FCoE traffic. QoS commands are for interfaces carrying non-FCoE traffic.

- HP recommends that Spanning Tree Protocol and its variants be disabled on CEE interfaces that are connected to a server.
- The Fabric Provided MAC Address (FPMA) and Fibre Channel Identifier (FCID) assigned to a VN_Port cannot be associated with any front-end CEE port on which the FLOGI was received.
- LLDP neighbor information may be released before the timer expires when DCBX is enabled on a CEE interface. This occurs only when the CEE interface state changes from active to any other state. When the DCBX is not enabled, the neighbor information is not released until the timer expires, regardless of the interface state.
- The FCoE login group name should be unique in a fabric-wide FCoE Login Management Configuration. The merge logic is designed to modify the login group name during merge when login group names in participating configurations conflict with each other. The Organizationally Unique Identifiers (OUI) of 00051E or 000533 (phased in beginning in April 2010) are being used by Brocade while assigning the WWNs to 2408 FCoE Converged Network Switches, DC SAN Backbone Directors, and DC04 SAN Directors, which would make only the last three bytes different for any two 2408 FCoE Converged Network Switches, DC SAN Backbone Directors, or DC04 SAN Directors. Considering this assignment method, the merge logic would rename the login group by including the last three bytes of the WWN in the login group name, so that they are unique in the merged configuration.
- For switches having different OUI indexes from the eight assigned to Brocade (for example, 00051E and 006069), WWNs can differ in more than three bytes. In this case, after a normal merge and a rename, per the logic described above, login group names can be the same for WWNs differing only in OUIs. The merge logic would drop one of the login groups to satisfy the requirement to keep the login group name unique in the fabric-wide configuration.
- Ethernet switch services must be explicitly enabled using the command `fosconfig –enable ethsw` before powering on a DC SAN Director Switch 10/24 FCoE Blade. Failure to do so causes the blade to be faulted (fault 9).
- To support nondisruptive firmware upgrades on the DC SAN Backbone Director/DC04 SAN Director, a new service, `ethsw`, is being introduced to enable Ethernet switching on the DC SAN Director Switch 10/24 FCoE Blade in Fabric OS 6.3. LAN switching is disabled by default in Fabric OS 6.3. The user must explicitly enable Ethernet switch service using the command `fosconfig –enable ethsw` to prevent FC traffic interruption.
- Upgrading DC SAN Backbone Director/DC04 SAN Director with DC SAN Director 10/24 FCoE blade from Fabric OS 6.x to 6.3 is nondisruptive. You can enable `ethsw` after upgrading without interrupting FC traffic. Upgrading firmware on the 2408 FCoE Converged Network Switch disrupts the FC traffic.
- For HP DC SAN or DC04 SAN Directors with one or more SAN Director Switch 10/24 FCoE blades installed, downgrading or upgrading the Fabric OS 6.3 firmware to another version disrupts traffic through the blades. HA Failover of CP blades in either of these directors disrupts traffic through the 10/24 FCoE blades.
- Upgrades from Fabric OS 6.3 to future releases will be nondisruptive to data traffic and will have behavior similar to a CP failover; `ethsw` remains unchanged.
- Downgrade from Fabric OS 6.3 to 6.1.2_cee1 is disruptive if `ethsw` is enabled on Fabric OS 6.3.
- Downgrade from Fabric OS 6.3 to 6.1.2_cee1 is nondisruptive if `ethsw` has never been enabled with Fabric OS 6.3.
- HA Failover of CP blades in DC SAN Backbone or DC04 SAN Director also results in disruption of traffic through the 10/24 blades.
- Connecting a 2408 FCoE Converged Network Switch to an FCR-capable switch with `fcrbcast config` enabled will cause a storm of broadcast traffic, resulting in termination of `iswitchd`.

- When rebooting a DC SAN director or DC04 SAN director with DC SAN 10/24 FCoE blade, Qlogic CNA and LSAN zoning, the switch becomes unresponsive for a period of time. This is due to the CNA sending excessive MS queries to the switch.
- A DC SAN 10/24 FCoE blade installed in the highest numbered slot of a DC SAN director or DC04 SAN director does not send out FIP unsolicited advertisements. Therefore, it does not support FCoE functionality when installed in this slot.

Virtual Fabrics

- On VF-capable platforms, the VF feature (initially supported with Fabric OS 6.2.0a) must be enabled in order to utilize the related capabilities, including logical switches and logical fabrics. Any switch shipped from the factory with 6.3.1a or later installed that is capable of supporting VF will have it enabled by default.
- When creating logical fabrics that include switches that are not VF-capable, it is possible to have two logical switches with different FIDs in the same fabric. Be sure to verify that the FIDs match for all switches in the same logical fabric.
- In order to support non-disruptive Hot Code Load on an HP 8/40 SAN Switch with VF enabled, the total zoning DB size for the entire chassis should not exceed 1 MB.
- A switch with VF enabled cannot participate in a fabric that uses IP filter or password database distribution or administrative domains. You must disable the VF feature before deploying it in a fabric that uses these features.
- VF is not supported on the 1606 Extension SAN switch.
- VF-dedicated ISLs are supported on the DC SAN Director Switch Multiprotocol Extension Blade. XISLs are not supported.
- On an HP 8/40 SAN switch with Virtual Fabrics enabled, ports may be re-initialized causing frame drops during a hot code load (HCL) if the switch has a zoning database that is 1MB or larger in size. To prevent this from occurring, ensure the zoning database is less than 1MB when activating new firmware.

Licensing behavior

When operating a switch with Fabric OS 6.3.*x*, some licenses may be displayed as `Unknown`. This is due to changes in licensing requirements for some features that no longer require a license key and may still be installed on a switch.

Adaptive Networking/flow-based QoS prioritization

- When using QoS in a fabric with 4-Gb ports or switches, Fabric OS 6.0 or later must be installed on all products in order to pass QoS information. E_Ports from the DC SAN Backbone

Director or DC04 SAN Director to other switches must come up after 6.0 is running on those switches.

- Flow-based QoS is not supported on any 8-Gb Fibre Channel blades in the 4/256 SAN Director.
- Any products that cannot operate with Fabric OS 6.x cannot exist in a fabric with flow-based QoS. Major problems occur if previous-generation 2-Gb products exist in the fabric.
- QoS is supported on switches in Access Gateway mode with Fabric OS 6.3x and later. The fabric switches should be running Fabric OS 6.3 to support QoS. If the fabric switch is Fabric OS 6.2, QoS must be disabled on either switch or AG. When running Adaptive Networking in Access Gateway mode, note the following:
  - QoS takes precedence over ingress rate limiting.
  - Ingress Rate Limiting is not enforced on trunked ports.

FCR backbone fabric ID changes

- With 8-Gb director blades, the switch must be disabled to change the backbone fabric ID.
- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.

Traffic Isolation over FCR

- All switches and Fibre Channel routers, both in edge and backbone fabrics, must be running Fabric OS 6.1.0 or later in order to support this feature.
- In order for TI over FCR to function properly, the associated TI zones in each fabric (edge and backbone) must have failover enabled.
- TI over FCR is supported only in edge-to-edge configurations. There is no support for TI in backbone-to-edge routing configurations.

IP over Fibre Channel (IPFC)/FCR

IPFC over FCR is now disabled by default. Switches that are upgraded to Fabric OS 6.3 will retain their configuration settings for IPFC over FCR. The change to the default configuration applies only to new units shipping with Fabric OS 6.3.1a or units running Fabric OS 6.3x that are reset to a default configuration. Use `fcrbcast --enable` to explicitly enable IPFC over FCR.

Broadcast frame forwarding in FCR fabric

Broadcast frame forwarding is not supported in an FCR fabric with a 2408 FCoE Converged Network Switch. By default, broadcast frame forwarding is disabled on the FC router. If your edge fabric includes a 2408 FCoE Converged Network Switch, do not enable broadcast frame forwarding on the FC router, which can degrade FCR performance when there is excessive broadcast traffic.

FC Routing with Mi10K

Using FC routing in a backbone-to-edge configuration with an Mi10k in the edge fabric, can result in slow throughput for hosts attached to the Mi10K following a bounced IFL connection between the backbone and edge fabric. To resolve this slowdown, disable and then re-enable the Mi10K ports for the affected hosts. Mi10k directors operating with firmware earlier than MEOS 9.9.5 may experience repeated system faults when attached as an FCR edge switch to a 1606 Extension SAN Switch EX_Port. To avoid this, ensure that the Mi10k is operating with MEOS 9.9.5 or later for this configuration.

Integrated routing

- To allow HCL on an 8/40 SAN Switch when using Integrated Routing, the edge switch connected to the 8/40 SAN Switch must be running Fabric OS 6.1 or later.
- Integrated Routing and Top Talkers cannot run concurrently in Fabric OS 6.3.x. To use Integrated Routing, be sure to disable Top Talkers before configuring EX_Ports.

FC FastWrite

When an FC FastWrite Initiator is moved to a port that does not have FC FastWrite enabled, I/O will recover and revert to the slow path route (non-FC FastWrite). This is a change from Fabric OS 6.2.x.

Native connectivity

Fabric OS-based platforms operating in interopmode 2 or 3 should never be deployed in a fabric without at least one M-series switch. Fabric OS switches in interopmode 3 (McDATA Open Fabric Mode) do not support configuration of zoning without an M-series switch in the fabric. When migrating from M-series to B-series switches, all B-series switches should be configured to interopmode 0 (Brocade Native mode) after the last M-series switch has been removed from the fabric.

M-EOSc switches may exhibit a behavior where they block all attached devices with a reason indication of `Blocked Temporarily, Internal`. This can occur when you power cycle the M-series switch while it was participating in a fabric with Frame Redirection zoning, a capability used for Fabric OS-based application or encryption services. If the switch is still participating in the fabric with Frame Redirection, issue the `cfgsave` command from a Brocade Fabric OS-based switch with the Frame Redirection zone in its defined zone database. If the M-EOS switch is no longer attached to the fabric with Frame Redirection zoning, issue the `Config.Zoning.deleteSplZoneSet` command via the CLI to the M-EOS switch.

FCS Automatic Distribution

- When using the FCS Automatic Distribution feature in Fabric OS 6.0 or later, all switches in the fabric must be running Fabric OS 6.0 or later. If any switches are running Fabric OS 5.x or earlier, only manual distribution can be used.
- Fabric OS 6.0 or later allows FCS Automatic Distribution only when in strict mode, requiring only switches with Fabric OS 6.0 or later.

FCAP

- Due to limitations with the certificates, FCAP authentication cannot be supported on user-defined logical switches. FCAP will continue to function with existing certificates for non-VF and the default logical switch of VF-enabled switches. Note that `authutil` is not restricted from other logical switches at this time, so it can still be enabled on unsupported LS.
- The pkicert (1.06) utility may cause `evm` errors, so each new switch should be isolated from the fabric in non-VF mode to install new certificates.
- For FIPS mode, certificates must be installed before FIPS activation.

FICON

NOTE: For information about specific versions of Fabric OS support for FICON, see the B-series FICON Connectivity Stream.

FL_Port (loop) support

- The 8-Gb 48-port Fibre Channel blade now supports the attachment of loop devices in the DC SAN Backbone Director and DC04 SAN Director.
- VF must be enabled on the chassis, and loop devices can be attached only to ports on a 48-port blade assigned to a nondefault logical switch operating with the default 10-bit addressing mode. (Loop devices may not be in the default logical switch.)
- A maximum of 144 ports can be used for connectivity to loop devices in a single logical switch in a chassis.
- Loop devices are supported when attached to ports on the 8-Gb and 4-Gb 16- and 32-port Fibre Channel blades, with no new restrictions.

Port Mirroring

- On the 8/80 SAN Switch, the Port Mirroring feature has a limitation where all port mirror resources must remain in the same ASIC port group. The resources are the configure mirror port, Source Device, and Destination Device or ISL, if the Destination Device is located on another switch. The ASIC port groups are 0-15, 16-31, 32-47, 48-63, and 64-79. The routes will be broken if the port mirror resources are spread over multiple port groups.
- Port Mirroring is not supported on the 1606 Extension SAN Switch.
- See the `portMirror` command in the Command Reference Guide for more information on mirror port configuration and requirements.

10Gb interoperability

10Gb interoperability between the HP SAN Director 6 Port 10Gb FC Blade and McDATA blades is not supported due to a hardware limitation. However, the SAN Director 6 Port 10Gb FC Blade is supported in a chassis running in interopmode 2 or 3 (SAN Director 6 Port 10Gb FC Blade to SAN Director 6 Port 10Gb FC Blade connections only). A SAN Director 6 Port 10Gb FC Blade will not synchronize with a McDATA 10Gb blade, but this will not negatively impact the system.

Port Fencing

- For Port Fencing, once the trigger threshold is exceeded (for example, for ITWs, CRCs, or LRs), Fabric Watch waits for approximately six seconds to see if the port is going offline. If it is still online at the next poll cycle, Fabric Watch fences the port. Extensive testing has shown that ports in the process of going offline may exhibit bursts of errors. Waiting the additional six seconds to check the port status helps prevent false positives and unnecessarily fencing a port (for example, during a server reboot).
- When using Port Fencing, you must first run the `fwalarmsfilterset` command. This command enables the port and allows you to receive Port Fencing messages.
- The state-changes counter used by Fabric Watch in Fabric OS 6.3 has been updated to ignore any toggling of F_Ports due to planned internal mechanisms, such as throttling and trunking. There are some Fabric OS CLI commands, such as `portcfgspeed` and `portCfgTrunkPort`, that implicitly disable/enable ports after configuration.
- Fabric Watch monitors state change for LISL ports, even though it is not displayed in Fabric Watch CLI commands.
- The Port Fencing feature is not supported for Loss of Sync (LOS) and Link Failure (LF) areas of Port/F_Port/E_Port classes. State change area can be used in place of LOS/LF areas for Port Fencing.

Zoning

Beginning with Fabric OS 6.2.0, all WWNs containing uppercase characters are automatically converted to lowercase when associated with a zone alias and stored as part of a saved configuration on a switch. For example, a WWN entered as either **AA.BB.CC.DD.EE.FF.GG.HH** or **aa.bb.cc.dd.ee.ff.gg.hh** when associated with a zone alias will be stored as `aa.bb.cc.dd.ee.ff.gg.hh` on a switch operating with Fabric OS 6.2.0 or later. This behavioral change in saved zone alias WWN members does not impact most environments. However, in a scenario where a switch with a zone alias WWN member with uppercase characters (saved on the switch with pre-Fabric OS 6.2.0 code) is merged with a switch with the same alias member WWN in lower case characters, the merge fails, since the switches do not recognize these zoning configurations as being the same. For additional details and workaround solutions, refer to the latest Fabric OS Administrator Guide.

ICLs

- If a DC SAN Director with an 8-link ICL license is connected to a DC SAN Director with a 16-link license, the DC SAN Director with the 16-link license will report `enc_out` errors. The errors are harmless, but will continue to increment. These errors will not be reported if a DC SAN Director with a 16-link license is connected to a DC04 SAN Director with only 8-link ICL ports.
- If ICL ports are disabled on only one side of an ICL link, the enabled side may see `enc_out` errors.

Extended Fabrics and R_RDY flow control

Starting with Fabric OS 5.1, the Extended Fabrics feature is supported with R_RDY flow control. (R_RDY flow control mode can be enabled using the `portCfgISLMode` command.) R_RDY flow control mode that uses IDLE primitives does not support frame-based trunking for devices such as Time Division Multiplexor (TDM). To overcome this limitation and provide support for frame-based trunking with Extended Fabrics, Fabric OS 6.2.x and later has been enhanced to support interoperability with these distance extension devices.

Fabric OS 6.3.0 and later allows Extended Fabrics E_Ports to operate in VC_RDY mode using either ARB or IDLE primitives as fill words. This allows frame-based trunking to be supported on Extended Fabrics E_Ports even when IDLE primitives are configured for these ports when operating in native VC_RDY mode. Prior to this change, frame-based trunking was supported only when ARB primitives were used in VC_RDY mode. With Fabric OS 6.2.x, frame-based trunking is supported on Extended Fabrics E_Ports even if IDLE or ARB primitives are used when operating in native VC_RDY mode.

Implementation

The `portcfglongdistance` CLI parameter `VC Translation Link Init` is now overloaded to specify whether the long-distance link should use IDLE or ARB primitives. By default `vc_init` is enabled. When `vc_init` is enabled, the long-distance link uses ARB primitives. When `vc_init` is disabled, the link uses IDLE primitives.

The buffer-to-buffer credit recovery feature is not supported on Extended Fabrics E_Port when it is configured to use IDLE primitives. The user must disable the buffer-to-buffer credit recovery feature using the `portcfgcreditrecovery` command and specifying the disable option; otherwise, the link will continuously reset.

The Adaptive Networking SID/DID Traffic Prioritization QoS feature is not supported on Extended Fabrics E_Ports when IDLE primitives are configured on these ports. In this mode, only data virtual channels are available when QoS-related virtual channels are not available.

When connecting to an extension device that does not support ARB primitives (such as some TDM products), the following configuration must be used:

- `portcfgqos -disable <port>`
- `portcfgcreditrecovery –disable <port>`
- `portcfglongdistance <port><LD|LD>0<distance>`

The fabric parameter `fabric.ops.mode.longdistance` is now deprecated and should not be used.

8-Gb link initialization and fill words

Overview

The Fibre Channel Physical Interfaces (FC-PI) standard defines the requirements for a physical layer. It considers all aspects of transmit, receive, and cable-plant performance requirements for optical and electrical links. The FC-PI standard has been modified to support new physical-layer variants that operate at higher data rates than those specified in FC-PI-2. The standard enables interoperability of transmitter devices, receiver devices, interconnects, and components from different manufacturers.

New variants include support for a data rate of 800 MB/s. The previous implementation by Brocade was to use Idles for link initialization and as fill words, which works for 1-Gb, 2-Gb, 4-Gb, and most 8-Gb devices. However, some of the new 8-Gb devices may require that the ARB(FF)/ARB(FF) sequence have successful link initialization. Brocade has developed an implementation of ARB(FF)/ARB(FF) for initialization and fill words. The `portcfgfillword` command, first introduced in Fabric OS 6.1.2, configures the ARB(FF)/ARB(FF) implementation. See the *Fabric OS Command Reference Manual supporting Fabric OS 6.3.1* for details on the `portcfgfillword` command.

`portcfgfillword` behavior summary

- **Default mode**

  The only mode of operation in releases prior to Fabric OS 6.1.2 was the Idle implementation. Fabric OS 6.2.0a and 6.2.0b defaulted to ARB(FF)/ARB(FF) for 8-Gb devices. With 6.1.2x and 6.2.0d and later, the default reverted to the Idle implementation. The `portCfgFillWord` command was also implemented beginning with these versions, and enables the user to configure the ARB(FF) configuration.

- **Existing product**

  For products in the field, this change has no effect on current configurations. The mode is currently 0, and during a firmware upgrade, the mode will remain 0 and no devices will be impacted. If a new device is added to the configuration, and it requires the ARB(FF) sequence, the ports can be configured at that time.

  Loading Fabric OS 6.1.2x or later does not automatically change the mode (with the exception of 6.2.0a and 6.2.0b, as noted above). In current configurations, the mode must be changed manually. This does not affect 1-Gb, 2-Gb, or 4-Gb devices. Any mode settings of 1, 2, or 3 have no effect on these devices; they affect only devices that negotiate or are fixed at 8-Gb speeds.

- **Changing the mode after Fabric OS 6.1.2x or later has been installed**

  If you change the mode after installing Fabric OS 6.1.2x or later, with the exception as noted above for 6.2.0a and 6.2.0b, the `portCfgFillWord` command changes the configuration parameter in accordance with the selected mode, and automatically disables/enables the port for which the command was invoked. Subsequent link initializations will default to the new mode setting.

- **Other scenarios**

  The `portCfgFillWord` command has no effect on 1-Gb, 2-Gb, or 4-Gb devices, but the mode is persistent. If a device attempts to negotiate or is fixed at 8 Gb, the configured mode will take effect. The persistent configuration is on a port-by-port basis; that is, if an 8-Gb device is connected to a 2-Gb or 4-Gb SFP, and that SFP is replaced with an 8-Gb SFP, then the current behavior of the mode is activated.

- The following table provides a `portcfgfillword` summary.

Fabric OS version	All 8-Gb switches except 8-Gb SAN Fabric OS version Switch for HP BladeSystem c-Class	8Gb SAN Switch for HP BladeSystem c-Class
Any Fabric OS earlier than 6.1.2	Any Fabric OS earlier than 6.1.2	All ports set to idle. No mode 1 capability existed. **NOTE:** Fabric OS 6.1.2 was not supported on this switch.
6.2.0x prior to 6.2.0c	The default setting for all ports is mode 1 and cannot be changed.	Default setting for all ports is mode 1 (internal and external) and cannot be changed.
6.1.2x and 6.2.0c and later (HP did not support 6.1.2c or 6.2.0c)	Added the ability to change `portcfgfillword` to mode 0 or mode 1 on a port-by-port basis.	Added the ability to change `portcfgfillword` to mode 0 or mode 1 on a port-by-port basis. **NOTE:** Fabric OS 6.1.2 was not supported on this switch.
6.1.2x and 6.2.0d through 6.3.0x	The default setting for all ports is mode 0, regardless of what Fabric OS version was previously installed. However, ports previously set to mode 1 by the user via the `portcfgfillword` command are persistent, and will therefore remain at mode 1 after Fabric OS upgrade.	◦ If version 6.2.0d was installed in the factory, the default setting is mode 1 for the internal ports and mode 0 for the external ports. The setting can be changed by the user on a port-by-port basis and will be persistent. Upgrading to a 6.3.0x version does not affect the current mode settings. ◦ If a pre-6.2.0d version was installed in the factory, the default setting for all internal and external ports is mode 0. The setting can be changed by the user on a port-by-port basis and will be persistent. Upgrading to one of the versions in the left column does not affect the current mode settings.
6.3.1a and later	Implemented support for modes 2 and 3 as described below. The default setting for all ports is mode 0, regardless of what Fabric OS version was previously installed. However, ports previously set to mode 1 by the user via the `portcfgfillword`	◦ If version 6.2.0d or 6.3.1c was installed in the factory, the default setting is mode 1 for the internal ports and mode 0 for the external ports. The setting can be changed by the user on a port-by-port basis and will be persistent. Upgrading

	command are persistent, and will therefore remain at mode 1 after Fabric OS upgrade.	to a version later than 6.3.1c does not affect the current mode settings. ◦ If a pre-6.2.0d version was installed in the factory, the default setting for all internal and external ports is mode 0. The setting can be changed by the user on a port-by-port basis and will be persistent. Upgrading to version 6.3.1a or later does not affect the current mode setting, with the exception of version 6.4.0b or later as described below. ◦ If upgraded to version 6.4.0b, regardless of what version was factory installed, all internal ports will be set to mode 1, and all external ports to mode 0. The setting can be changed by the user on a port-by-port basis and will be persistent.
Modes	0—Idle for link init, idle for fill word 1—Arb(ff) for link init, arb(ff) for fill word (not supported with EVA or XP storage arrays) 2—Idle for link init, arb(ff) for fill word 3—Initially attempts mode 1 link initialization. If unsuccessful in achieving active state, reverts to mode 2. Steady state fill word is arb(ff). (not supported with XP storage arrays earlier than Fabric OS 6.4.0a.)	

Miscellaneous

- The severity of RASLOG message AN-1003 has been raised from WARNING to ERROR in Fabric OS 6.3.2c and later 6.3.x releases. This change allows customers to easily trap on the event via SNMP. AN-1003 is not an actual error but an indication that there may be a potential bottleneck device attached to the switch. Customers who do not want to be notified of this RASLOG event should leave Bottleneck Detection disabled.
- POST diagnostics for the 8/40 SAN switch have been modified in Fabric OS 6.3.1b/6.4.0 and later releases to eliminate an `INIT NOT DONE` error at the end of an ASIC diagnostic port loopback test. This modification addresses BL-1020 initialization errors encountered during the POST `portloopbacktest`. During non-disruptive firmware upgrades, E_Ports in R_RDY mode may cause some frame drops on the E_Port links.
- Modem capability for the 4/256 director is not supported in Fabric OS 6.2.0 and later.
- On the HP 8/8, 8/24, 8/40, and 8/80 SAN Switches with factory installed Fabric OS 6.3.1a, the assignment of PIDs (FCIDs) is non-deterministic. The area field of the PIDs is assigned the first time the switch is booted up, based on the order that ports are recognized and brought up by the system. Switch PIDs area will not be equal to port number, which may impact servers such as FICON or static PID bind servers that need area equal to port numbers to log in to the fabric successfully. To avoid this issue, customers can bind PIDs using the `portaddress --bind [slot_number/]port_number [16-bit_address]` command prior to allowing devices to log in to the switch. Once assigned, the PIDs are maintained across reboots and future Fabric OS upgrades. This issue does not impact switches that do not have Fabric OS 6.3.1a factory installed. Field upgrade to a later version of Fabric OS will not resolve this situation. For environments in which this will be an issue, the specified workaround will need to be implemented until a future version of Fabric OS is factory installed.
- Beginning with Fabric OS 6.2.0, the data collected by `SupportSave` operations was greatly expanded to include all readable registers within the ASIC. In cases where some registers may be unused and therefore contain invalid data, a CDR-1003 error message would be

issued. Fabric OS 6.3.1b and later now reclassifies these messages as warnings, rather than critical errors.

- A new command has been introduced in Fabric OS 6.3.2a that allows configuration of the fault delay on individual ports. The command `portCfgFaultDelay` allows a port to be configured to a 1.2 second fault delay versus the default setting of R_A_TOV.
  - **NAME:** `portCfgFaultDelay` - Configures the fault delay for a single FC port.
  - **SYNOPSIS:** portcfgfaultdelay [slot/]port, mode
  - **DESCRIPTION:** Use this command to configure the fault delay of an FC port. In the event that the link is noisy after a host power cycle, the switch may go into a soft fault state, which means a delay of R_A_TOV. Setting the mode value to 1 reduces the fault delay value to 1.2 seconds. The configuration is stored in nonvolatile memory and is persistent across switch reboots and power cycles. Use the `portCfgShow` command to display user-configured fault delay settings.

Encryption behavior

- HP recommends that the encrypted LUN containers be created when all of the nodes/encryption engines (EEs) in the Data Encryption Key (DEK)/High Availability Cluster (HAC) are up and enabled.
  - If two Encryption Engines are part of a High Availability Cluster, configure the host/target pair such that they form a multipath from both EEs. Avoid connecting both the host/target pairs to the same EE. This connectivity does not give full redundancy in case of EE failure resulting in HAC failover.
  - Since the quorum disk plays a vital role in keeping the cluster in sync, configure the quorum disk to be outside of the encryption environment.
- LUN configuration
  - To configure a LUN for encryption:
    - Add the LUN as clear-text to the Crypto Target Container (CTC).
    - When the LUN comes online and the clear-text host I/O starts, modify the LUN from clear-text to encrypted, including the `enable_encexistingdata` option to convert the LUN from clear-text to encrypted.
  - An exception to this LUN configuration process: If the LUN was previously encrypted by the HP Encryption Switch or HP Encryption Blade, the LUN can be added to the CTC with the `–encrypt` and `–lunstate ="encrypted"` options.
  - LUN configurations must be committed to take effect. No more than 25 LUNs can be added or modified in a single commit operation. Attempts to commit configurations that exceed 25 LUNs will fail with a warning. There is also a five-second delay before the commit operation takes effect.

    Always ensure that any previously committed LUN configurations or LUN modifications have taken effect before committing additional LUN configurations or additions. All LUNs should be in an Encryption Enabled state before committing additional LUN modifications.
- The `cryptocfg -manual_rekey -all` command should not be used in environments with multiple encryption engines (encryption blades) installed in a director-class chassis when more than one encryption engine has access to the same LUN. In such situations, use the `cryptocfg -manual_rekey <CTC> <LUN Num> <Initiator PWWN>` command to manually rekey these LUNs.
- If an HA Cluster is configured within an Encryption Group with containers configured for `auto` Failback Mode, the following procedure must be followed when upgrading from Fabric OS

6.2.x to 6.3.2. Note that the following procedure is required only under the above-mentioned conditions.

1. Before the firmware upgrade, change the Failback Mode to `manual` for all containers configured as `auto`. Take note of which Encryption Engines currently own which containers.
2. Upgrade all nodes in the Encryption Group to Fabric OS 6.3.2, one node at a time.
3. After all nodes have been successfully upgraded, using the notes taken in step 1, manually invoke the failback of the containers to the correct Encryption Engine using the command `cryptocfg -failback -EE <WWN of hosting node> [slot num] <WWN of second node in HAC> [slot num].`
4. Once the manual failback completes, change the Failback Mode back to `auto` from `manual`, if it was changed in step 1.

- Avoid changing the configuration of any LUN that belongs to a CTC/LUN configuration while the rekeying process for that LUN is active. If the user changes the LUN's settings during manual or auto, rekeying or First Time Encryption, the system reports a warning message stating that the encryption engine is busy and a forced commit is required for the changes to take effect. A forced commit command halts all active rekeying processes running in all CTCs and corrupts any LUN engaged in a rekeying operation. There is no recovery for this type of failure.
- Configuration of crypto targets on HP encryption switches or encryption blades is accomplished in two stages: entering the configuration changes and issuing a commit operation. Previous to Fabric OS 6.3.1a, if the data encryption group (Encryption Group) became incomplete (one or more members became inaccessible due to network problems and the encryption group becomes "degraded") between these two stages, the commit operation was still executed. While this did not result in any issue for the configured host and targets, it could lead to configuration changes being applied to only a subset of the encryption switches in the encryption group. This was a rare situation that had only been seen in test environments. This issue has been resolved in Fabric OS 6.3.1a.
- If the data encryption group (Encryption Group) gets into a state where the Group Leader encryption switch reports that another encryption switch is NOT a member node of the encryption group, and the encryption switch member node still indicates that it IS part of the encryption group, the following recovery action can be performed to re-merge the nodes into the encryption group:

  1. On the Group Leader encryption switch, execute the CLI command `cryptocfg –dereg –membernode <WWN of member node>`
  2. Wait for 30 seconds.
  3. Execute the CLI command `cryptocfg –reg –membernode <WWN membernode> <certificate file name> <ipaddr of member node>`

  This is a rare situation that has been noted in a test environment where there were intermittent management network connectivity problems. A fix for this issue is in the Fabric OS 6.4.0 release.

- To remove access between a given initiator and target, the user must not only remove the active zoning information between the initiator and target, but must also remove the associated CTCs, which will in turn remove the associated frame redirection zone information. Make sure to back up all data before taking this action.
- Before committing configurations or modifications to the CTC or LUNs on an HP Encryption Switch or HP Encryption Blade, make sure that there are no outstanding zoning transactions in the switch or fabric. Failure to do so results in the commit operation for the CTC or LUNs failing and may cause the LUNs to be disabled. The user can check for outstanding zoning transactions by issuing the CLI command `cfgtransshow`:

```
DCX_two:root> cfgtransshow
```

```
There is no outstanding zoning transaction
```

- Each LUN is uniquely identified by the HP Encryption Switch or HP Encryption Blade using the LUN's serial number. The LUN serial numbers must be unique for LUNs exposed from the same target port. The LUN serial numbers must also be unique for LUNs belonging to different target ports in nonmultipathing configurations. Failure to ensure unique LUN serial numbers results in nondeterministic behavior and may result in faulting of the HP Encryption Switch or HP Encryption Blade.
- When creating an HA cluster or EG with two or more HP Encryption Switch/Encryption Blades, the GE ports (I/O sync links) must be configured with an IP address for the `eth0` and `eth1` Ethernet interfaces using `ipaddrset`. In addition, the `eth0` and `eth1` Ethernet ports should be connected to the network for redundancy. These I/O sync links connections must be established before any Re-Key, First Time Encryption, or enabling EE for crypto operations. Failure to do so results in HA Cluster creation failure. If the IP address for these ports is configured after the EE was enabled for encryption, HP Encryption Switch needs to be rebooted and Encryption Blades should be `slotpoweroff/slotpoweron` to sync up the IP address information to the EEs. If only one Ethernet port is configured and connected to a network, data loss or suspension of Re-Key may occur when the network connection toggles or fails.
- `initEE` will remove the existing master key or link key. Backup the master key by running `cryptocfg –exportmasterkey` and `cryptocfg –export –currentMK` before running `initEE`. After `initEE`, `regEE` and `enableEE`, run `cryptocfg –recovermasterkey` to recover the master key previously backed up, or in the case of fresh install run `cryptocfg – genmasterkey` to generate a new master key. If you are using SKM, establish a trusted link with SKM again. Certificate exchange between key vaults and switches are not required in this case.
- The disable EE interface CLI `cryptocfg --disableEE [slot no]` should be used only to disable encryption and security capabilities of the EE from the Fabric OS Security Admin in the event of a security compromise. When disabling the encryption capabilities of the EE using the noted commands, the EE should not be hosting any CTCs. Ensure that all CTCs hosted on the HP Encryption Switch or HP Encryption Blade are either removed or moved to a different EE in the HA Cluster or EG before disabling the encryption and security capabilities.
- Whenever `initNode` is performed, new certificates for CP and KAC (SKM) are generated. Hence, each time `InitNode` is performed, the new KAC Certificate must be loaded onto key vaults for (SKM. Without this step, errors will occur, such as key vault not responding and ultimately key archival and retrieval problems.
- The HTTP server should be listening to port 9443. SKM is supported only when configured to port 9443.
- Configuring a Brocade group on SKM: As described in the *Fabric OS Encryption Administrator's Guide*, a Brocade group needs to be configured on SKM (under Local Users & Groups) for managing all keys generated by Brocade encryption switches and blades. It is important to note that the name for this group is case sensitive and must be "brocade," not "Brocade."
- When all nodes in an EG (HA Cluster or DEK Cluster) are powered down (due to catastrophic disaster or a power outage to the data center) and later nodes come back online (in the event of the Group Leader (GL) node failing to come back up or the GL node being kept powered down) the member nodes lose information and knowledge about the EG. This leads to no

crypto operations or commands (except node initialization) being available on the member nodes after the power-cycle. This condition persists until the GL node is back online.

- **Workaround.** In the case of a data center power down, bring the GL node online first, before bringing the other member nodes online.

  In the event of the GL node failing to come back up, the GL node can be replaced with a new node. The following are the procedures to allow an EG to function with existing member nodes and to replace the failed GL node with a new node.

- **Make one of the existing member nodes the Group Leader node and continue operations.**
  1. On one of the member nodes, create the EG with the same EG name. This will make that node the GL node and the rest of the CTC and Tape Pool related configurations will remain intact in this EG.
  2. For any containers hosted on the failed GL node, issue `cryptocfg --replace` to change the WWN association of containers from the failed GL node to the new GL node.

- **Replace the failed GL node with a new node.**
  1. On the new node, follow the switch/node initialization steps.
  2. Create an EG on this fresh switch/node with the same EG name as before.
  3. Perform a `configdownload` to the new GL node of a previously uploaded configuration file for the EG from an old GL node.
  4. For any containers hosted on the failed GL node, issue `cryptocfg --replace` to change the WWN association of containers from failed GL node to the new GL node.

- During an online upgrade from Fabric OS 6.2.0x to 6.3.2, we expect to see the I/O link status reported as `Unreachable` when the `cryptocfg` command is invoked. However, once all the nodes are upgraded to Fabric OS 6.3.2, the command will accurately reflect the status of the I/O Link. The I/O link status should be disregarded during the code upgrade process.
- The `–key_lifespan` option has no effect for `cryptocfg –add –LUN`, and only has an effect for `cryptocfg --create –tapepool` for tape pools declared `-encryption_format native`. For all other encryption cases, a new key is generated each time a medium is rewound and block zero is written or overwritten. For the same reason, the **Key Life** field in the output of `cryptocfg --show -container -all –stat` should always be ignored, and the **Key Life** field in `cryptocfg --show –tapepool –cfg` is significant only for native-encrypted pools.
- The Quorum Authentication feature requires DCFM 10.3.0 or later. Note that all nodes in the EG must be running Fabric OS 6.3.0 or later for quorum authentication to be properly supported.
- In a DC SAN Director or DC04 SAN Director with Fabric OS 6.3.2 and DC Switch encryption FC blades installed, you must set the quorum size to zero and disable the system card on the blade prior to downgrading to a Fabric OS version earlier than 6.3.0.
- The System Card feature requires DCFM 10.3.0 or later. Note that all nodes in the EG must be running Fabric OS 6.3.0 or later for system verification to be properly supported.
- The Encryption SAN Switch and Encryption FC blade do not support QoS. When using encryption or Frame Redirection, participating flows should not be included in QoS Zones.
- HP encryption devices can be configured for either disk or tape operation. The ability to configure multiple Crypto-Target Containers defining different media types on a single encryption engine (Encryption SAN Switch or Encryption FC blade) is not supported until Fabric OS 6.4.0. Encryption FC blades can be configured to support different media types within a common DC SAN Director/DC04 SAN Director chassis.

- SKM is supported with Multiple Nodes and Dual SKM Key Vaults. Two-way certificate exchange is supported. See the Encryption Admin Guide for configuration information. If you are using dual SKMs on Encryption SAN Switch/Encryption FC blade Encryption Group, these SKM Appliances must be clustered. Failure to cluster will result in key creation failure. Otherwise, register only one SKM on the Encryption SAN Switch/Encryption FC blade Encryption Group.
- When the tape key expires in the middle of write operation on the tape, the key is used to append the data on the tape media. When the backup application rewinds the media and starts writing to Block-0 again (and if the key is expired), a new key is created and used henceforth. The expired key is then marked as read only and used only for restoring data from previously encrypted tapes.
- With Windows and Veritas Volume Manager/Veritas Dynamic Multipathing, when LUN sizes less than 400 MB are presented to the Encryption SAN Switch for encryption, a host panic may occur; this configuration is not supported for Fabric OS 6.3.x.
- HCL from Fabric OS 6.2.x to 6.3.2 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 traffic will not be.
- Relative to the Encryption SAN Switch and a DC SAN Director with Encryption FC blade, all nodes in the Encryption Group must be at the same firmware level of Fabric OS 6.2 or 6.3 before starting a rekey or First Time Encryption operation. Make sure that existing rekey or First Time Encryption operations complete before upgrading any of the encryption products in the Encryption Group. Also, make sure that the upgrade of all nodes in the Encryption Group to Fabric OS 6.3.2 completes before starting a rekey or First Time Encryption operation.
- To clean up the stale rekey information for the LUN, use one of the following methods:
  - **Method 1**
    1. Modify the LUN policy from `encrypt` to `cleartext` and commit.

       The LUN will become disabled.
    2. Enable the LUN using `cryptocfg --enable –LUN`. Modify the LUN policy from `clear-text` to `encrypt` with `enable_encexistingdata` to enable the first time encryption and do commit.

       This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption.
  - **Method 2**
    1. Remove the LUN from Crypto Target Container and commit.
    2. Add the LUN back to the Crypto Target Container with `LUN State="clear-text"`, `policy="encrypt"` and `enable_encexistingdata` set for enabling the First Time Encryption and commit.

       This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption.

- In an environment with a mixed firmware version (Fabric OS 6.2.x + 6.3.x) Encryption Group, the I/O link state reported for Fabric OS 6.2.x nodes is unreachable. During a rolling upgrade from Fabric OS 6.2.0x to 6.3.2, you should see the I/O link status reported as `Unreachable` when the `cryptocfg –show -loc` command is invoked. However, once all the nodes are upgraded to Fabric OS 6.3.2, the show command will accurately reflect the status of the I/O Link. The I/O link status while performing the rolling upgrade from Fabric OS 6.2.x to 6.3.2 can be ignored until all nodes have been upgraded to 6.3.2.

```
Mace39:root> cryptocfg --show -loc

    EE Slot:                    0
       SP state:                Online
       Current Master KeyID:    43:f1:bd:dc:91:89:f2:f1:6a:a1:48:89:7b:d0:5f:59
       Alternate Master KeyID: 3a:a4:5b:86:90:d5:69:26:29:78:f8:3b:f9:b2:9c:b9
       HA Cluster Membership:   hac39_115
```

```
        EE Attributes:
            Link IP Addr   : 10.32.50.36
            Link GW IP Addr: 10.32.48.1
            Link Net Mask  : 255.255.240.0
            Link MAC Addr  : 00:05:1e:53:8a:86
            Link MTU       : 1500
            Link State     : UP
            Media Type     : DISK
            System Card Label    :
            System Card CID      :

Remote EE Reachability :

Node WWN/Slot                          EE IP Addr      EE State
IO Link State
10:00:00:05:1e:53:77:80/0       10.32.53.107    EE_STATE_ONLINE          Non-Reachable
10:00:00:05:1e:53:b7:ae/0       10.32.53.105    EE_STATE_ONLINE          Non-Reachable
```

- SKM FIPS Mode Enablement

  FIPS compliance mode is disabled in SKM by default. To enable it, follow the procedure described in the SKM user guide, “Configuring the Key Manager for FIPS Compliance” section.

  NOTE: Per FIPS requirements, you cannot enable or disable FIPS when there are keys on the Key Manager. Therefore, if FIPS enablement is required, HP strongly recommends that it be performed during the initial SKM configuration, before any key sharing between the switch and the SKM occurs.

- SKM dual node cluster - Auto failover considerations:

  In a dual node SKM cluster configuration with the encryption switch, ensure that the two SKM nodes are always available and online for proper key archival. If one of the SKM nodes fails, you cannot use the configuration to create new keys. In other words, adding new targets or LUNs to the encryption path will not work until both the SKM nodes are available. However, there will not be any issue for retrieving keys or using the existing setup as long as one SKM node is available.

  The encryption switch ensures that any new KEY is hardened (archived) to both SKM Key Vaults in the SKM Cluster before the key gets used for encryption. In the event that one of the SKM vaults is down, the key creation fails because of the hardening check failure. As a result, the new key creation operation will not function. For Key retrieval, this is not the requirement and any one Key Vault being online will get the Key as long as that Key Vault has the Key.

Initial setup of encrypted LUNs

IMPORTANT: While performing first-time encryption to a LUN with more than one initiator active at the time, rekey operations slow to a standstill. Define LUNs for a single initiator at a time to avoid this occurrence.

NOTE: When configuring multipath LUNs, care should be taken to add LUN 0 on all of the paths, subject to the following considerations:

- If LUN 0 presented by the back-end target is a controller LUN (not a disk LUN; that is, not visible in the `discoverLUN` output), add LUN 0 to the container as a clear text LUN. Make sure all of the paths have this LUN 0 added for MPIO operation (EVA configuration, for example).
- If LUN 0 presented by the back-end target is a disk LUN, LUN 0 can be added to the container either as clear text or encrypted (MSA configuration, for example).
- For HP-UX, LUN 0 can appear as 0x0 or 0x400, but both of them are LUN 0 only and should be treated alike.

Documentation Updates

This section provides information on last minute additions and corrections to the documentation. The most recent Fabric OS 6.3 documents are available on www.hp.com in the "manuals" section for switches that support that version of Fabric OS (the “manuals” section is accessible once you navigate to a particular switch). The updates noted in this section are in addition to those included in the previous Fabric OS 6.3.0x Release Notes. There are no additional documentation updates for this version of release notes.

NOTE: The *Fabric OS FCIP Administrator Guide* and *Fabric OS Command Reference* documents are updated to reflect new support and changes in Fabric OS 6.3.1.

Brocade Fabric OS Command Reference (Publication Number 53-1001337-01)

The `cryptoCfg` command description and associated man page should be updated as follows: On pages 148 and 149, under the “Storage device configuration and management” function of the `cryptoCfg` command, two new parameters have been added to the `--add` and `--modify –LUN` commands.

```
cryptocfg --add -LUN crypto_target_container_name LUN_Num | LUN_Num_Range
[initiator_PWWN initiator NWWN [initiator_PWWN initiator NWWN]...]
[-lunstate encrypted | cleartext] [-keyID keyID]
[-encryption_format native | DF_compatible]
[-encrypt | -cleartext] [-enable_encexistingdata | -disable_encexistingdata]
[-enablerekey time_period | -disable_rekey]
[-key_lifespan time_in_days | none]
New parameters:
  [-write_early_ack disable | enable]
   [-read_ahead disable | enable]
```

```
cryptocfg --modify -LUN crypto_target_container_name LUN_Num initiator_PWWN
[-encryption_format native | DF_compatible]
[-encrypt | -cleartext]
[-enable_encexistingdata | -disable_encexistingdata]
[-enablerekey time_period | -disable_rekey]
New parameters:
  [-write_early_ack disable | enable]
   [-read_ahead disable | enable]
```

Add the following parameter descriptions on page 160 for the `--add –LUN` and on page 161 and `--modify -LUN` commands:

`-write_early_ack` `disable | enable`

Specifies the Tape Write pipelining mode of the LUN. This option enables or disables early acknowledgement of commands (internal buffering) for a tape LUN. This feature is enabled by default.

`-read_ahead` `disable | enable`

Specifies the Tape Read Ahead mode of the LUN. When Tape Read Ahead is disabled, the tape LUN operates in unbuffered mode. When Tape Read ahead is disabled, the tape LUN operates in buffered mode. This feature is enabled by default.

Brocade Fabric OS Encryption Administrator’s Guide (Publication Number 53-1001760-011001341-02)

Add the `–write_early_ack` and `-read_ahead` parameters to Table 8, “LUN Parameters and Policies” on page 113.

Fabric OS 6.3.2 fixes

“Fabric OS 6.3.2 fixes” (page 40) lists defects closed in the Fabric OS 6.3.2 firmware release.

Table 6 Fabric OS 6.3.2 closed defects

Closed defect summary	Solution
A switch panic occurs during `firmwaredownload` with termination of msd (management server daemon). If a request was cancelled in the midst of processing, a race condition between two threads can occur, triggering an msd panic and `hareboot/hafailover` of switches. Observed in fabric with EOSc switch that ignores GMAL request.	Fixed in Fabric OS 6.3.2.
The `firmwarerestore` command does not restore the firmware to the original version after a `firmwaredownload` to downgrade from Fabric OS 6.4.x to 6.3.x, or from Fabric OS 6.3.x to 6.2.x with the `-sfbn` option	**Workaround prior to upgrade:** Manually reboot the switch after `firmwarerestore`. Fixed in Fabric OS 6.3.2.
As a result of `firmwaredownload`, `systemverifcation` test, or blade insertion, occasionally 10/24 FCoE blade may turn faulty 21.	**Workaround prior to upgrade:** Use `slotpoweroff/on` the 10/24 FCoE blade to clear the faulty state. Fixed in Fabric OS 6.3.2.
Intermittent network connection problem led to failure of the management interface port on the encryption SAN switch, causing multiple switches within the encryption group to go out of sync. The encryption Group Leader detected the departure of a member, but the member did not detect the departure of the Group Leader, and the group got out of sync.	Fixed in Fabric OS 6.3.2.
After moving a 10/24 FCoE director blade from slot 1 to slot 2 in a DC SAN Backbone director, and a CP failover, CNAs are not able to login.	Fixed in Fabric OS 6.3.2.
Directors with 8Gb blade in slot 1 or 8Gb switches see frame drop in the fabric when there are Ex/VEx ports configured in the same ASIC chip as an F/E port with EGID 0. Fabric with this problem can be identified by running `sloterrshow 1` on directors or `sloterrshow` on a switch, and `type6_miss` counter should be seen continuously incrementing during traffic load on backend port/E_Port.	**Workaround prior to upgrade:** Avoid configuring an EX_Port or a VE_Port near an F/E_Port with an EGID of 0. To identify a port with an EGID of 0, login as root and run `bladeportmap [1]`. The first port where `Upt` is not `-1` uses EGID 0. Once the problem occurs, the user must make the F/E port into an EX_Port and then configure it back to an F/E_Port to fix the problem port. Execute the following instructions: 1. Disable the F/E_Port. 2. Configure the F/E_Port as an EC_Port for a valid FID. 3. Connect a link between the FID and the EX port (IFL). 4. Enable the port. 5. Verify that the link is online, then disable the port. 6. Disable the EX_Port configuration. 7. Connect the host/ISL back to the F/E_Port. 8. Enable the port. Fixed in Fabric OS 6.3.2.
Switch reboot after Access Gateway daemon panic following hot code load (HCL). This failure is usually observed with [PORT-1003] in raslog, and only with Access Gateway enabled switches.	Fixed in Fabric OS 6.3.2.
Very intermittent issue where rpcd crash can occur due to uninitialized pointer, if user changes security configuration (certificates or rpc secret) through Web Tools while there is an active rpc connection from SMI-A. Due to this rpcd panic followed by `weblinker.fcg` restart to make the configuration effective, a cold recovery of the CPs is triggered.	**Workaround prior to upgrade:** Stop using the SMI-based application until the firmware is upgraded to Fabric OS 6.3.2. Fixed in Fabric OS 6.3.2.

Table 6 Fabric OS 6.3.2 closed defects *(continued)*

Access Control Lists are not getting populated, even though the ACL Policies are set on the switch. As a result, ACL related configuration is not possible through DCFM or other common access layer (CAL) interfaces, even though it can be done through the CLI. This issue affects only the HP 2408 FCoE switch and 10/24 FCoE blade.	**Workaround prior to upgrade:** Use the CLI. Fixed in Fabric OS 6.3.2.
CNA cannot login during shut/no shut of port that occurs in the middle of FCoE login attempt. Doing fcoe `-enable/disable` does not recover it. This issue affects only the HP 2408 FCoE switch and 10/24 FCoE blade.	Fixed in Fabric OS 6.3.2.
After a `firmwaredownload hafailover/hareboot`, switch is missing domain route, indicated by RTWR-1003 retry messages. Only pertinent to fabric with VE link to 1606 Extension SAN switch or Multiprotocol Extension blade in IM2 mode.	Fixed in Fabric OS 6.3.2.
A device with a node WWN of zero connected to an NPIV port that is queried by CALD, causes the switch to panic and reboot about every 20 to 30 minutes.	Fixed in Fabric OS 6.3.2.
With a switch in Access Gateway mode, a few ports were observed as persistently disabled after enabling QoS on all trunked F_Ports, with the message: `Area of those ports had been acquired by the ports that were not in the same trunk`. Occurs when port SCNs come in an unexpected order.	Fixed in Fabric OS 6.3.2.
A switch panic occurs during reboot due to a race condition caused by a data structure not yet being allocated by a daemon and yet another daemon querying it. Applies only to the 2408 FCoE switch and 10/24 FCoE blade.	Fixed in Fabric OS 6.3.2.
Routes are not being properly rebalanced after a trunk group loses a member, which could lead to sluggish performance on 8Gb switches if there is a slow drain device using the lower bandwidth link to further congest the fabric.	**Workaround prior to upgrade:** Keep trunk groups with equal bandwidth. Fixed in Fabric OS 6.3.2.
Detected termination of zoning daemon process during `firmwaredownload`. Race condition triggered the zoning daemon to access unintialized global memory and then crash.	Fixed in Fabric OS 6.3.2.
May see frame drops on some device ports and E_Ports after `hafailover`. E_Port change SCN event or fabric unstable event results in fspf routing protocol incorrectly mapping slave to master port or incorrectly programming interface IDs on the trunks. Frames are routed to the wrong port and dropped.	**Workaround prior to upgrade:** May need to block and unblock all ports in the trunk to recover from the rare condition. Fixed in Fabric OS 6.3.2.
FCR matrix specifies which FCR pairs can talk to each other. All edge fabrics connected to the defined pair of FCRs are allowed to import devices to each other. However, after a fabric event, FCR did not handle domain unreachable SCN timing sequence correctly, leading to the FCR matrix information being out of sync among all FCRs in the fabric; all imported disks went to configured.	**Workaround prior to upgrade:** Disable FCR matrix by issuing the following commands: 1. `fcrlsanmatrix -remove -fcr wwn wwn` 2. `fcrlsanmatrix -apply -fcr` Fixed in Fabric OS 6.3.2.
WWN PID static binding was setup on the switch using the `wwnaddress -bind` command and WWN_A is bound to PID A, and WWN_B is bound to PID B. Almost instantaneously, both ports go offline due to a device "rebalance" and, when the links come back up, WWN to PID binding is swapped. Ports become disabled with the reason `Disabled (PPID set on device, other port online with area)`.	Fixed in Fabric OS 6.3.2.
As a result of an external FC port on the encryption SAN switch or blade experiencing an excessive number of encoding CRC errors, the internal ports are faulted incorrectly by switch firmware. This leads to a data encryption virtual initiator associated with the internal port failing to appear in the name server.	**Workaround prior to upgrade:** Remove the condition/cause of the excessive CRC errors (that is, replace cable or SFP). Fixed in Fabric OS 6.3.2.

Table 6 Fabric OS 6.3.2 closed defects *(continued)*

Rolling asserts occur on 4/256 SAN Director with Multiprotocol Router blade, or on 400 Multiprotocol Router when attempting to connect to an encryption SAN switch via EX_Port.	**Workaround prior to upgrade:** Disable the E_Port on the encryption switch to recover the switch. Fixed in Fabric OS 6.3.2.
PLOGI ACC is dropped when there is back-to-back `plogin` to a well-known address such as msd, nsd, fabric controller, etc., before the switch route setup is completed. The PLOGIs are held in queue without being ACC'd until the route setup is completed, but the issue is that once the setup is done, only one of the PLOGIs is ACC'd and the rest are dropped. Applies to any switch running 6.x Fabric OS, but more likely in directors. This is an unlikely scenario, because most devices do not perform such back-to-back logins early during switch/fabric bring up.	Fixed in Fabric OS 6.3.2.
During a stress test where interface toggling was triggered while a login is pending, a kernel panic occurred on the 2408 FCoE switch or 10/24 FCoE blade.	Fixed in Fabric OS 6.3.2.
When F_Port trunking is activated and after the master trunk goes offline, the switch adds the new master trunk to the list of ports, which will send EFP/BF/DIA flood. The ports remain in this state until all N_Ports are taken offline and logged back into the fabric again. Build Fabric (BF) is sent to the AG. AG forwarding the BF to redundant fabric caused fabric disruption.	Fixed in Fabric OS 6.3.2.
iSCSI director blade `iscsicfg -commit all` hangs the switch Telnet session, and `hafailover` is needed to recover.	Fixed in Fabric OS 6.3.2.
Weblinker terminated while removing slot-based license. 1. Open the switch via http and get into the licenseadmin page, **Switchadmin -> licenseadmin.** 2. Remove the Advanced extension slot based license. Weblinker is terminated. The daemon is restarted without further functional impact.	Fixed in Fabric OS 6.3.2.
With VF disabled, aborts and timeouts were seen on traffic over FCIP of FID 128 when Port Based Route Policy (aptpolicy of 1) was not propagated from CP to DP properly.	Fixed in Fabric OS 6.3.2.
With an invalid http configuration on 4Gb switches, after step upgrading from Fabric OS 5.3.1x to Fabric OS 6.2.x, switch (or standby CP on 4/256 director) ends up in panic loop, and may remain in perpetual reboot state. This occurs when there is an inconsistency between SSL certificate and http configuration.	**Workaround prior to upgrade:** Manually ensure that `http.enabled` matches with SSL certificate by `configshow http.enabled` as admin user. If inconsistent with SSL certificate requirement, execute `/fabos/libexec/webdconfigure` as root to set "HPPT Enable" to yes. Or schedule a window, disable switch, and `configdownload` a file with `http.ebale:1 [end]` when switch is at Fabric OS 5.3.x or 6.1.x to correct the configuration. If switch is already stuck in a reboot loop, login as root via serial console, copy and paste the following command string into the console as one line before the next reboot: `sed 's/http.enabled:0/http.enabled:1/g" tmp;cp tmp/etc/fabos/fabox.0.conf;cp tmp/mnt/etc/fabos/fabos.0.conf;rm tmp` Fixed in Fabric OS 6.3.2.

Table 6 Fabric OS 6.3.2 closed defects *(continued)*

CALD terminated and logical switch delete failed with reason `Could not get port details from EM` when attempting to delete two of six logical switches in a DC SAN Backbone director from DCFM.	Fixed in Fabric OS 6.3.2.
In AG mode, N_Port failover results in F_Ports with attached hosts getting stuck as G_Ports. Occurs when there is a change in the base address for the N_Port due to failover, or when there is no wwn-area mapping for few devices and due to the login sequence of these devices. The PIDs assigned conflicted with the already allocated PID to another device, resulting in the F_Ports getting stuck as G_Ports.	Fixed in Fabric OS 6.3.2.
Large core file fills up the compact flash and causes file system corruption. If Fabric OS startup files are corrupted, the switch ends up in a reboot loop.	Fixed in Fabric OS 6.3.2.
QoS circuits running over a 1 Gb/10 Gb bandwidth circuit on 1606 Extension switch or Extension blade will have incorrect QoS distributions with large I/O. Occurs when running all three QoW priorities on a circuit that is a multiple of 1 Gb/s and effects the distribution of traffic, which could lead to performance issue.	Fixed in Fabric OS 6.3.2.
Webd was seen to terminate from time to time, at the same time as HA status temporarily went to non-redundant, triggering a Call Home event. Webd was killed by a watchdog as it was waiting for a reply from a busy httpd and did not have a timeout mechanism. No other functional impact observed other than Call Home event.	Fixed in Fabric OS 6.3.2.
Multiple FCR masters in edge fabrics after ISL issues in the backbone.	**Workaround prior to upgrade:** Triggering a warm boot on the switch that should not be FCR master (higher WWN) should trigger it to recalculate the FCR master. Fixed in Fabric OS 6.3.2.
After firmware upgrade to Fabric OS 6.3.x, SNMP V3 requests are not returned with correct values and V3 traps are not received.	Fixed in Fabric OS 6.3.2.
FICON Tape Emulation aborts from channel due to incorrect CCW number in generated command retry status for write conv busy sequences. Channel Detected Error messages are seen for FICON Emulated tape devices during tape pipelining, leading to some special tape media (WORM drives) being unusable.	**Workaround prior to upgrade:** Disable FICON Emulation. Fixed in Fabric OS 6.3.2.
64 bit port stats are available only in CLI via `portStats64Show`, not exposed through SNMP. Need to enhance SNMP code to expose these counters.	Fixed in Fabric OS 6.3.2.
Created a TI zone followed by `cfgsave` and `cfgenable`; `zone -show` indicated that it was created, but later reissuance of `zone -show` did not display the TI zone.	Fixed in Fabric OS 6.3.2.
TI zone with failover-disabled policy under base switch is not supported and needs to be blocked. There are overlapping TI zones with failover-disabled policy under LS partition in which one uses DISL connection and the other uses XISL connection. When DISL connection gets disabled, there is no traffic going through the XISL connection.	**Workaround prior to upgrade:** Do not use TI zone with failover-disabled policy under base switch. With the code change in this release, executing TI zone command with failover-disabled policy under base switch gets the response: `Cannot create TI zone with failover flag disabled on a base switch.` Fixed in Fabric OS 6.3.2.
The 1606 Extension switch does not support the Path Down function in IM2 mode. Fabric becomes unstable and segments when one leg of a TI Zone with Failover Disabled is disrupted.	Fixed in Fabric OS 6.3.2.

Table 6 Fabric OS 6.3.2 closed defects *(continued)*

In an encryption environment, tape devices intermittently show `offline` condition to the host. Observed in setup where some Physical Initiators do not register as FC4 type devices and some do.	Fixed in Fabric OS 6.3.2.
On 4Gb switches, when a frame comes into the embedded port and there is no memory to hold it temporarily, the switch panics. This is likely to happen when there are spurious interrupts from a device.	Fixed in Fabric OS 6.3.2.
When `FCP_CONF` command is dropped, the restore job from tape is unable to continue and complete successfully. Applies only to the 1606 Extension switch and Multiprotocol Extension blade.	Fixed in Fabric OS 6.3.2.
CP-1250 heartbeat is dead on Multiprotocol Router blade, which results in a CP panic and reboot.	Fixed in Fabric OS 6.3.2.
If per port NPIV limit on AG is set to greater than 26, some F_Ports may not come online and stay as G_Ports.	Fixed in Fabric OS 6.3.2.
The `configdefault` command on the switch is not setting default fcmap to 0x0efc00. If `configdefault` is issued after `slotpoweroff` or after removing a blade from a slot, `configdefault` can fail without setting the default value for fcmap, thereby not returning the switch to the default factory state. This affects the 2408 FCoE switch and 10/24 FCoE blade only.	Fixed in Fabric OS 6.3.2.
Open SSL is updated to address CVD-2009-3555/CERT advisory 120541 (TLS and SSL protocol vulnerability).	Fixed in Fabric OS 6.3.2.
Tape drives fail when running over FCR with EX_Ports in Open mode. The REC accept payload is incorrect. If host to tape I/O traverses FCR and includes an edge fabric, the tape drives run for a bit and then fail because REC ACC is not processed correctly if the EX_Port is operating in IM3/Open mode.	Fixed in Fabric OS 6.3.2.
ARP goes away and Neighbor Discovery timeouts occur on routed networks after pulling GE cables during heavy traffic. No end-to-end connection can be established. Tunnel 20 (GE4) failed to recover. Switch had to be reset to recover.	Fixed in Fabric OS 6.3.2.
With tape encryption, backup to all clear text containers using `netbackup` in a Multiplex/stream environment results in an encryption SAN switch fault, causing tape flows to halt.	Fixed in Fabric OS 6.3.2.
Tunnel creation failed with error message `Unable to add more FCIP circuits to this tunnel` when using VE_Ports 12-15 on DC SAN Backbone director with 2 or more Multiprotocol Extension blades. Not an issue with DC04 SAN director or 1606 extension switch.	**Workaround prior to upgrade:** Use VE_Ports 16-31. Fixed in Fabric OS 6.3.2.
Unable to disable default zone from Mi10k in interop fabric in IM2 mode after zone merge failure.	Fixed in Fabric OS 6.3.2.
Bottleneckmon cannot be enabled on F_Ports with `Locked G_Port` and `Disabled E_Port` enabled in `portcfg`.	**Workaround prior to upgrade:** Disable either or both "Locked G_Port" and "Disabled E_Port" features, but note that this operation is disruptive. Fixed in Fabric OS 6.3.2.
Abort in FICON Tape Read emulation if Attention status is received between status and status accept.	**Workaround prior to upgrade:** Disable FICON emulation. Fixed in Fabric OS 6.3.2.

Fabric OS 6.3.2a fixes

Table 7 (page 46) lists defects closed in the Fabric OS 6.3.2a firmware release

Table 7 Fabric OS 6.3.2a closed defects

Closed defect summary	Solution
In a fabric containing the encryption switch and/or encryption blade, numerous weblinker termination and restart messages can be seen due to timeouts in handling multiple stats calls in parallel.	Fixed in Fabric OS 6.3.2a.
After doing a firmware upgrade or an hafailover on a 4/256 director with 4Gb 48 port blade installed, the CP blade faults and traffic is disrupted. External RASLOG EM-1051 messages are seen, reporting a slot inconsistency detected. This can occur if a PLOGI is received right before the hafailover or hot code load and it has zone misses for devices communicating through the primary shared area port.	Fixed in Fabric OS 6.3.2a.
Port zoning enforcement cycles between session based zoning and hard zoning. This can happen when name server queries occur at the same time as a zone configuration change is initiated. ZONE-1004 messages are seen in RASLOGs but no traffic interruption is observed. Applies to all platforms.	Fixed in Fabric OS 6.3.2a.
When standby CP is not responsive (stuck in reboot loop) on any director class switch, Weblinker causes the active CP to reboot, leading to a cold recovery.	Fixed in Fabric OS 6.3.2a.
FICUD ASSERT/auto-reboot occurs when changing logical switch configuration due to random timing condition in accessing switch configuration data. Observed when running `lscfg` commands to configure FICUD ports. Both CPs reboot with disruptive recovery.	Fixed in Fabric OS 6.3.2a.
Race condition in FCP daemon logging mechanism causes memory corruption and panic. This leads to cold recovery during firmware download or when management applications using the SMI client continuously query the switch. Occurs in VF configurations with multiple logical switches configured running Fabric OS 6.2.x and 6.3.x previous to 6.3.2a only.	**Workaround prior to upgrade:** Perform hafailover/hareboot to clean up any existing corruption before code upgrade, then disable FCP logging using fcplogdisable to avoid any further corruption until upgrading to a version of Fabric OS with the fix. Fixed in Fabric OS 6.3.2a.
During host reboot, F_Port may come up as G_Port on 4/8, 4/16, 4Gb switch for HP p-Class BladeSystem or 4Gb switch for HP c-Class BladeSystem.	Fixed in Fabric OS 6.3.2a.
Compact Flash (CF) can sometimes fail silently. In such cases, the user sees only critical daemon failures triggering a failover. Sometimes no failure is seen, and the switch continues running but does not produce any logs. Fabric OS 6.3.2a provides an enhancement to CF failure handling to detect and proactively trigger an hafailover when a bad part is detected.	Fixed in Fabric OS 6.3.2a.
On 8Gb switches, constant link resets occur when a long distance E_Port port is configured that requires 128 to 511 credits. These link resets occur continuously with no traffic, and a constant stream of C2-5021 indications are seen.	**Workaround prior to upgrade:** Use OOS mode. Fixed in Fabric OS 6.3.2a.
Host ports can experience slow performance after enabling and then disabling Top Talker. Class 3 frame rejects can also be seen in the portlogdump. This is due to a residual setting in the firmware that causes class 3 frame rejects to be continuously forwarded to the CPU causing the slow performance.	Fixed in Fabric OS 6.3.2a.
Switch panics, blade faults, or switches getting disabled when credit loss is detected on internal backend port. RASLOG C-5021 or C2-5021 indications are reported.	Fixed in Fabric OS 6.3.2a.
Fabric Watch FW-1186 and FW-1190 messages are logged with values above 100%. Likely to occur during first Fabric Watch polling cycle after slotstatsclear command has been issued.	Fixed in Fabric OS 6.3.2a.
Traffic routed through an 8Gb 48 port blade in a DC SAN Backbone director running Fabric OS 6.3.0 through 6.3.2 will be misrouted following an HA failover. HA failover can be triggered in numerous ways including a firmware upgrade. When this occurs in this configuration, the DCX misroutes traffic	**Workaround prior to upgrade:** Bounce affected primary port or move device off the secondary shared area port. Fixed in Fabric OS 6.3.2a.

Table 7 Fabric OS 6.3.2a closed defects *(continued)*

on a primary shared area port after a secondary shared area F_Port goes though a route recalculation. Level of disruption varies from causing a SCSI abort, RTWR error, to hosts and targets losing the ability to communicate.	
Fabric gets into a mode where communications between the local switch and remote switch flow in only one direction, causing the remote switch to disable the local switch without any notification or reason being logged. Messages are seen indicating RTWR has reached max retries in RASLOG.	Fixed in Fabric OS 6.3.2a.
Multi-sequence frames are not properly handled by switches in Access Gateway mode, leading to memory corruption and switch agdd panic.	Fixed in Fabric OS 6.3.2a.
Formatting of errdump messages resulting from changes made to support virtual fabrics causes some firmware upgrade log messages related to the previously installed version of Fabric OS to be lost after upgrade to Fabric OS 6.2.0 or later.	Fixed in Fabric OS 6.3.2a.
Haenable command is not auto rebooting the standby CP when the standby CP is removed and reseated/replaced. As a result the active and backup CP end up out of synch. Can occur with either 4Gb or 8Gb director class switches.	**Workaround prior to upgrade:** Reboot the standby CP manually. Fixed in Fabric OS 6.3.2a.
A multiple critical CDR-1003 raslog occurred during supportsave. After a non-disruptive upgrade from Fabric OS 6.1.x to Fabric OS 6.2.x, CDR-1003 CRITICAL messages may be posted during a supportSave operation on Brocade 4Gb platforms. With the fix in this release, the critical message is updated to a Warning and it can be ignored unless it is persistent and does not occur during supportsave.	**Workaround prior to upgrade:** Ignore if CDR-1003 occurs during supportsave and is not persistent. Fixed in Fabric OS 6.3.2a.
With some types of servers that do not cut off the light during reboot, the connected switch cannot bring an F_Port on line for a long time due to multiple reinitialization attempts caused by unstable signal/port fault period.	Fixed in Fabric OS 6.3.2a.
Network security vulnerabilities identified via network vulnerability scan need to be addressed with the encryption switch and blade.	Fixed in Fabric OS 6.3.2a.
Newly active CP fails to completely recover from either firmware download (6.2.x to 6.3.x) or hafailover, due to persistent disabled GE_Port on Multi-protocol router blade. Requires a reboot of both CPs to regain hasync. Can occur with either 4Gb or 8Gb director class switches.	Fixed in Fabric OS 6.3.2a.
On Multi-protocol router blade or 400 MP router, after a TCP/FCIP processor panic, the CP panics with a "Oops: kernel access of bad area" message when attempting to output RASLOG messages.	Fixed in Fabric OS 6.3.2a.
In 8Gb FCR fabrics, If a switch performs an HA failover at the same time as a device in the fabric is continuously issuing a PLOGI to ports that are not online (due to device caching old PIDs and blindly doing login attempts to these PIDs periodically), the switch may drop SCSI command frames across IFL connections after hafailover, while SCSI data frames pass through. This does not happen with normal device plogin to devices already in the name server database, and affects 8Gb FCR only.	**Workaround prior to upgrade:** Remove the device issuing the PLOGI to offline ports from the fabric to avoid the problem. Fixed in Fabric OS 6.3.2a.

Fabric OS 6.3.2b fixes

Table 8 (page 47) lists defects closed in the Fabric OS 6.3.2b firmware release

Table 8 Fabric OS 6.3.2b closed defects

Closed defect summary	Solution
In a dual Inter-fabric Link (IFL) FCR fabric with LSAN Matrix configured and LSAN binding enabled, disabling the EX_Port for one of the IFLs causes all FCR devices to be removed from the name server database.	Fixed in Fabric OS 6.3.2b.
The `Tape REC` command fails in an FCR environment because the originator source ID in the header and in the body of the `TAPE REC` command frame	Fixed in Fabric OS 6.3.2b.

Table 8 Fabric OS 6.3.2b closed defects *(continued)*

do not match, causing the command to fail and resulting in data corruption on the tape.	
The fans on an HP DC SAN Backbone Director Switch may erroneously be flagged as bad and get logged with a `[PLAT-5042], FAN I2C reset` error code in the Raslog, even though they are operating properly.	**Workaround prior to upgrade:** Reseat the fans to allow them to recover from the faulty state. Fixed in Fabric OS 6.3.2b.
The `Switchshow` command reports the switch port state as "Mod_Val" rather than "Online" after a switch reboot test and ISL fails to form. This applies to all switches except the HP 8/8 Base (0) e-port SAN Switch, HP 8/8 (8)-ports Enabled SAN Switch, HP 8/24 Base 16-ports Enabled SAN Switch, HP 8/40 Base 24-ports Enabled SAN Switch, and the HP 8/40 Power Pack+ 24-ports SAN Switch.	Fixed in Fabric OS 6.3.2b.
Tape backups fail intermittently when there are multiple FCRs connected to the same edge fabric. This is caused by failure to translate the Proxy PID in the ACC payload of a TAPE REC command.	Fixed in Fabric OS 6.3.2b.
Weblinker processes terminate with a core dump and then restart when querying Top Talker information from a switch.	Fixed in Fabric OS 6.3.2b.
On 8 Gb platforms, a host on the backbone FCR is unable to discover its targets after an HA failover or code upgrade occurs on the backbone FCR. This is caused by the Domain table routing entry accidentally being cleared on an EX_Port after `hafailover`, preventing the backbone hosts from discovering their targets.	Fixed in Fabric OS 6.3.2b.
On the HP Encryption SAN Switch, kacd crashes and the switch reboots during online rekey and HA Cluster `failover/failback`.	Fixed in Fabric OS 6.3.2b.
CRC errors on internal links might occur on the HP 2408 24-10GbE w/8-8Gb FC Base FCoE and HP 2408 24-10GbE w/8-8Gb PwrPk+ FCoE Switches when jumbo frames are transmitted under certain traffic loads below the full line rate. If extensive CRC errors occur, traffic may stop completely and port `disable/enable` may be required to restore affected user ports.	Fixed in Fabric OS 6.3.2b.
Customers may be unable to upgrade from Fabric OS 6.2.0x to 6.3.x on an HP 4/256 SAN Director with an HP B-Series Multi-protocol Router Blade when a GE port is present and is persistently disabled. The CP could end up with an invalid configuration after attempting recovery by again downgrading to Fabric OS 6.2 and rebooting. This action could prevent the CP from successfully upgrading. Additionally, a good CP with a valid configuration that is HA synced with this CP could also be affected by the misconfigured CP.	**Workaround prior to upgrade:** Enable all persistently disabled GE ports prior to the first upgrade. If a downgrade has already been performed, execute a `configremove` of the invalid configuration and download a valid configuration to restore the CP. Fixed in Fabric OS 6.3.2b.
Switch Route (RTE) failures cause traffic issues or switch panics.	Fixed in Fabric OS 6.3.2b.
The `supportshow/supportsave` operations executed after a fastboot may cause SCSI timeouts to occur on the following switches: • HP 8/8 Base (0) e-port SAN Switch • HP 8/8 (8)-ports Enabled SAN Switch • HP 8/24 Base 16-ports Enabled SAN Switch • HP 8/80 Base 48-ports Enabled SAN Switch • HP 8/80 Power Pack+, 48-ports SAN Switch • HP 1606 SAN Extension Switch • HP EVA4400 embedded switch module, 8Gb Brocade • Brocade 8Gb SAN Switch for HP BladeSystem c-Class Class 3(C3) frame discards occur due to destination unreachable. However, since only a very small number of frames are dropped and the server retries SCSI traffic, users will not experience any functional impact.	Fixed in Fabric OS 6.3.2b.

Table 8 Fabric OS 6.3.2b closed defects *(continued)*

In an AG fabric, DXFM/FM/SMI proxy switch sends a GAGI request to another switch in the fabric with Brocade_AG query. This sometimes triggers verify and floods the raslog, which may cause high CPU load and switch panic.	Fixed in Fabric OS 6.3.2b.
With Virtual Fabrics (VF) enabled and Radius server configured, customers may see RAS-1004 Software 'Verify' errors logged every 3 minutes on each VF on a switch being managed by DCFM or Web Tools. The errors fill the RASLOG and eventually cause an FFDC event in other system modules due to “too many open files”. Virtual Fabrics can be configured on the following switches: • HP DC SAN Backbone Director Switch PP • HP DC04 SAN Director Switch • HP 8/80 Base 48-ports Enabled SAN Switch • HP 8/80 Power Pack+, 48-ports SAN Switch • HP 8/40 Base 24-ports Enabled SAN Switch • HP 8/40 Power Pack+ 24-ports SAN Switch	Fixed in Fabric OS 6.3.2b.
SW MIB counters such as Link Error State Block, Port Level Performance/Error, and other similar objects are available through CLI commands, but not through SNMP.	Fixed in Fabric OS 6.3.2b.
Tape performance is degraded after a tape drive has been idle for a few hours and then traffic is restarted on an HP 1606 SAN Extension Switch.	Fixed in Fabric OS 6.3.2b.
Users are unable to create a Certificate Signing Request (CSR) on a switch with only an IPv6 address configured.	Fixed in Fabric OS 6.3.2b.
The output of the `switchstatusshow` command reports an invalid switch status rather than the "marginal" status when application blades go down. This is caused by the Fabric Watch blade handler monitor mishandling the status of application blades.	Fixed in Fabric OS 6.3.2b.
Fabric Watch reports TX/RX performance over 100% after executing the `statsclear` command.	**Workaround prior to upgrade:** Use the `slotstatsclear` command instead of the `statsclear` command. Fixed in Fabric OS 6.3.2b.
The LED for online trunked F_Ports goes from a steady green to off after a code upgrade or `hareboot/hafailover`.	Fixed in Fabric OS 6.3.2b.
For both portstats and SNMP MIB output commands, counters quickly wrap on GE_Ports of an HP 1606 SAN Extension Switch or an HP DC SAN Director Multiprotocol Extension Blade.	Fixed in Fabric OS 6.3.2b.

Fabric OS 6.3.2c fixes

Table 9 (page 49) lists defects closed in the Fabric OS 6.2.3c firmware release.

Table 9 Fabric OS 6.3.2c closed defects

Closed defect summary	Solution
Frames received on shared area port trunks are improperly routed on an HP SAN Director 48-port 8Gb FC Blade in an HP DC SAN Backbone Director. This may occur after the remote trunk master goes offline and then comes back online.	Fixed in Fabric OS 6.3.2c.
A switch panic/director HA Failover may occur due to resource contention when TopTalker is monitoring traffic flows.	Fixed in Fabric OS 6.3.2c.
Customers are unable to access a device after FCIP links bounce multiple times. Frames with same SID/DID were sent to the device after the proxy translation failed in a backbone to edge FCR setup.	Fixed in Fabric OS 6.3.2c.

Table 9 Fabric OS 6.3.2c closed defects *(continued)*

Closed defect summary	Solution
After upgrading a fabric switch from Fabric OS from 6.2.x to 6.3.x, the N_Port was stuck in G_Port when the fabric switch is attached to an Access Gateway switch with QoS enabled.	Fixed in Fabric OS 6.3.2c.
FAN frames are not being sent by the switch to loop devices after LIP when fcAL.fanFrameDisable is set to 0.	Fixed in Fabric OS 6.3.2c.
A reboot of a host on one port group may adversely affect another host in a different port group causing loss of connectivity to their storage.	Fixed in Fabric OS 6.3.2c.
A switch with busy management applications may run into a race condition when more than one RPC connection gets established simultaneously. This may cause multiple connections to free a shared object twice and trigger an rpcd panic.	Fixed in Fabric OS 6.3.2c.
Access Gateway trace data lacks enough information for path loss debugging.	Fixed in Fabric OS 6.3.2c.
SW MIB counters such as Link Error State Block, Port Level Performance/Error, and other similar objects are available through the CLI but not through SNMP.	Fixed in Fabric OS 6.3.2c.
After a device performs a LOGO, followed by port offline and online events, the switch route is not properly re-established, and the host cannot discover targets.	Fixed in Fabric OS 6.3.2c.
Due to an incorrect internal counter logic, PORT-1003 port faults are erroneously being reported in the RASLOG.	Fixed in Fabric OS 6.3.2c.
After configuring the SCC Policy only on an edge switch, then removing the front domains of the FCR from the SCC followed by disabling/enabling the edge switch, the F_Ports get disabled with the following message: `2010/08/20-16:19:45, [SEC-1187], 1433, FID 128, INFO, T5300_161, Security violation: Unauthorized switch 20:00:00:05:1e:0a:54:ca tries to join fabric.`	Fixed in Fabric OS 6.3.2c.
There is currently no functionality to disable the IPv6 interface when duplicate addresses are detected.	Fixed in Fabric OS 6.3.2c.
Customers may experience false fan related errors on the HP 2408 24-10GbE w/8-8Gb FC Base FCoE Switch.	Fixed in Fabric OS 6.3.2c.
SNMP shows MIB connUnitPortEntries only for ports that have SFPs installed.	Fixed in Fabric OS 6.3.2c.
Kernel panic encountered while accessing compact flash.	Fixed in Fabric OS 6.3.2c.
Pv6 named Certificate Signing Request (CSR) files may not be FTP'd to some Windows based ftp server because of the presence of "." in the filename.	Fixed in Fabric OS 6.3.2c.
Customers may observe a temporary laser fault with SFPs, or other I2c access retries during heavy load.	Fixed in Fabric OS 6.3.2c.
After replacing a drive on an FL_Port, the initiator cannot discover the device. The newly replaced device on the Loop port does not register with name server properly.	Fixed in Fabric OS 6.3.2c.
When BE credit is lost, customers need to reseat the blade to recover.	Fixed in Fabric OS 6.3.2c.
seccertutil genkey reports "Configure a Valid IPv4 or IPv6 address" when there already is a valid IPv6 address.	Fixed in Fabric OS 6.3.2c.
The severity for the RASLOG AN-1003 error is raised from WARNING to ERROR in order to provide an easy interface for customers to trap it through SNMP. Customers who do not want to see this RAS log should leave Bottleneck Detection disabled.	Fixed in Fabric OS 6.3.2c.
If SNMP polling by management application is too frequent, the CPU may become overloaded resulting in other operational failures not directly related to this functionality.	Fixed in Fabric OS 6.3.2c.

Table 9 Fabric OS 6.3.2c closed defects *(continued)*

Closed defect summary	Solution
There previously was no easy way to diagnose link level errors on backend ports. This release includes a new diagnostic command, pterrshow, to display ASIC backend errors.	Fixed in Fabric OS 6.3.2c.
Ports cannot negotiate at 8G speed on the following switches: • HP 8/8 Base (0) e-port SAN Switch • HP 8/8 (8)-ports Enabled SAN Switch • HP 8/24 Base 16-ports Enabled SAN Switch • HP 8/80 Base 48-ports Enabled SAN Switch • HP 8/80 Power Pack+, 48-ports SAN Switch • HP EVA4400 embedded switch module • 8Gb Brocade Brocade 8Gb SAN Switch for HP BladeSystem c-Class • HP 1606 SAN Extension Switch	Fixed in Fabric OS 6.3.2c.
Issuing an HA failover command on either of the HP SN8000B SAN Backbone Directors (8-Slot or 4-Slot) may result in internal routing related errors for ICL ports.	Fixed in Fabric OS 6.3.2c.

Fabric OS 6.3.2d fixes

Table 10 (page 51) lists defects closed in the Fabric OS 6.2.3d firmware release.

Table 10 Fabric OS 6.3.2d closed defects

Closed defect summary	Solution
Upon disabling one link of a two-port trunk, the HP DC SAN Backbone Director Switch encountered both CPs panicking within three minutes. This is a topology and upgrade path specific issue.	Fixed in Fabric OS 6.3.2d.
Hosts may lose access to storage after changing the FCR backbone domain ID on an HP DC SAN Backbone Director Switch or HP DC04 SAN Director Switch with an HP SAN Director 48-port 8Gb FC Blade or an HP DC SAN Director 64-port 8Gb FC Blade. The frames drops occur on the backend ports of the blades.	Fixed in Fabric OS 6.3.2d.
A switch running in Access Gateway (AG) mode does not clean up the fabric channel frame exchange properly. This occurs when FLOGI/FDISC comes in from different ports together with same exchange ID (OX-ID).	Fixed in Fabric OS 6.3.2d.
A host is unable to access the target when connected to a 4 Gb switch during a specific storage device power-up sequence.	Fixed in Fabric OS 6.3.2d.
SNMP Throttling commands are not available for admin user.	Fixed in Fabric OS 6.3.2d.

Fabric OS 6.3.2e fixes

Table 11 (page 51) lists defects closed in the Fabric OS 6.2.3d firmware release.

Table 11 Fabric OS 6.3.2e closed defects

Closed defect summary	Solution
A switch panic may occur when there are GE_Ports with SFPs installed on an HP DC SAN Director Multiprotocol Extension Blade or an HP 1606 SAN Extension Switch.	Fixed in Fabric OS 6.3.2e.
An unstable link may trigger continuous timeout/discard frame/un-routable frame tracing to the CPU for processing on the HP StorageWorks 4/256 SAN Directors.	Fixed in Fabric OS 6.3.2e.

Table 11 Fabric OS 6.3.2e closed defects *(continued)*

Closed defect summary	Solution
Migration failures may occur between servers when a switch running in Access Gateway mode does not clean up the fabric channel frame exchange properly. This occurs when a FLOGI/FDISC is received from different ports with same exchange ID (OX-ID).	Fixed in Fabric OS 6.3.2e.
Excessive (encoding out) port errors may occur on HP 8/8 or 8/24 SAN Switches ISL ports in a configuration consisting of a mix of 4 Gb user ports interconnected via 8 Gb ISLs.	Fixed in Fabric OS 6.3.2e.
An HA Failover and reboot may occur during a code upgrade when an F_Port goes down and stays offline.	Fixed in Fabric OS 6.3.2e.
A host may be unable to link up to an 8 Gb FC port when it is set to a fixed speed of 4Gb or 8Gb.	Fixed in Fabric OS 6.3.2e.
During HA Failover, there is a potential for losing credits when there are too many timed-out and unrouteable frames being forwarded to the CPU.	Fixed in Fabric OS 6.3.2e.
The HP 8/40 SAN Switch, HP SAN Director 6-port 10Gb FC Blade, and the HP DC SAN Director Multiprotocol Extension Blade may experience a large number of CRC errors.	Fixed in Fabric OS 6.3.2e.
An HA Failover on the HP StorageWorks 4/256 SAN Director with any HP StorageWorks DC SAN Director FC Blade (16-port, 32-port or 48-port) installeld may result in a rare race condition, and a reset of the port blades may cause temporary traffic disruption. Customers may experience intermittent CRC errors when performing large data transfers from third-party tape drives on encrypted products, which may result in data read failures.	Fixed in Fabric OS 6.3.2e.
A switch panic occurs and Access Gateway may crash upon receiving bad frames (ELS_LOGO with SID 0) from devices.	**Workaround prior to upgrade:** Avoid sending LOGO with SID 0 to Access Gateway. Fixed in Fabric OS 6.3.2e.
Unreliable speed negotiations may occur with Brocade 5470 switches when connected to non-Brocade HBAs.	Fixed in Fabric OS 6.3.2e.
When doing `firmwaredownload -s` with HA disabled and auto reboot enabled on a backup CP, hot code load (HCL) will fail with the message `HCL failed. Please use reboot to reboot the switch manually`.	Fixed in Fabric OS 6.3.2e.
The Ethernet port sometimes sends frames with an invalid Ethernet MAC address on an HP 8/40 SAN switch, HP 1606 SAN Extension Switch, and HP SN6000B 16Gb FC Switch. This has no functional impact because TCP/IP retransmits the frames successfully. However, if security software is monitoring each frame, it will trigger alarms upon detection of an invalid MAC address.	**Workaround prior to upgrade:** Use 100 Half duplex instead of Full Duplex mode. Fixed in Fabric OS 6.3.2e.
EZ manager should allow custom zoning when a dual configured device exists in the switch.	**Workaround prior to upgrade:** Use Advanced Management web tools instead of EZ manager. Fixed in Fabric OS 6.3.2e.

Effective date

March 2012